BLANK FOR CHIEF'S PREFACE

Preface

Change in law enforcement is both constant and imminent. As Sheriff of the Madison County Sheriff's Office, I feel a profound sense of humility and pride in the opportunity to share in this growth with each of you. It is truly through your daily dedication, vigilance, and commitment to the citizens we serve that we are able to accomplish the vision set forth in our Mission Statement.

A fundamental component of earning public trust includes not only transparency but also the ability to form partnerships under which the safety and security of our community will continue to flourish. Such are our aspirations in the publication of this policy manual. Our great nation was founded upon principles of inalienable rights, and the authority vested upon us as law enforcement officers to abridge those rights necessitates acting within the framework of established jurisprudence. This framework would be incomplete without the establishment of policies to provide guidance thereby ensuring law enforcement service in a consistent and just manner to all.

The standards of conduct to which we hold ourselves responsible as outlined herein govern not only the aspects of our day-to-day operations, but also form the foundation of our service and accountability to the citizens we serve. With this policy manual, we continue an ongoing process of advancement and growth as a professional law enforcement agency and re-affirm our commitment to making this a department in which every member should be proud.

It is the responsibility of all employees of this department to become familiar with the rules, regulations, policies, and procedures set forth in this manual. The manual will be distributed via e-mail to all personnel and will always be available on the Network. The failure of an employee to know the contents of this manual will not be a defense in the case of any member considered for disciplinary action for a violation of any of the provisions contained herein. In situations that are not specifically addressed in this manual, it is expected that all personnel will act with good judgment, common sense, and in a manner generally consistent with the purpose of this manual.

Adherence to this manual is critical to the overall success of our department. It will provide us with assistance in gauging our effectiveness while serving to hold each of us accountable for our actions and activities. It stands as an immediate resource document ready to assist all members of our organization in accomplishing the goals of our stated mission.

As your Sheriff, I am honored to serve with a group of professionals who commit themselves daily to serving with honor, pride, and dignity. Thank you for the opportunity to serve.

Erik J. Weaver
Sheriff

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

LAW ENFORCEMENT CODE OF ETHICS

As a law enforcement officer, my fundamental duty is to serve the community; to safeguard lives and property; to protect the innocent against deception, the weak against oppression or intimidation and the peaceful against abuse or disorder; and to respect the constitutional rights of all to liberty, equality and justice.

I will keep my private life unsullied as an example to all and will behave in a manner that does not bring discredit to me or to my agency. I will maintain courageous calm in the face of danger, scorn or ridicule; develop self-restraint; and be constantly mindful of the welfare of others. Honest in thought and deed both in my personal and official life, I will be exemplary in obeying the law and the regulations of my department. Whatever I see or hear of a confidential nature or that is confided to me in my official capacity will be kept ever secret unless revelation is necessary in the performance of my duty.

I will never act officiously or permit personal feelings, prejudices, political beliefs, aspirations, animosities or friendships to influence my decisions. With no compromise for crime and with relentless prosecution of criminals, I will enforce the law courteously and appropriately without fear or favor, malice or ill will, never employing unnecessary force or abuse and never accepting gratuities.

I recognize the badge of my office as a symbol of public faith, and I accept it as a public trust to be held so long as I am true to the ethics of police service. I will never engage in acts of corruption or bribery, nor will I condone such acts by other police officers. I will cooperate with all legally authorized agencies and their representatives in the pursuit of justice.

I know that I alone am responsible for my own standard of professional performance and will take every reasonable opportunity to enhance and improve my level of knowledge and competence.

I will constantly strive to achieve these objectives and ideals, dedicating myself before God to my chosen profession . . . law enforcement.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

BLANK FOR MISSION STATEMENT

Vision

The Madison County Sheriff's Office is responsible for protecting constitutional guarantees and impartially enforcing the law. We believe that integrity is the basis of
public trust and that honesty and equality in the delivery of services is essential. We commit ourselves to uphold these values and to foster cooperation and respect within our community.

Mission Statement

The mission of the Madison County Sheriff's Office is to serve and protect all citizens in a respectful, compassionate, and professional manner while protecting human dignity in every circumstance. We value and expect truth, honesty, and ethical behavior from the members of our organization. We are committed to upholding our position of public trust by maintaining the highest ethical standards and the utmost respect for the laws of our county, state, and nation. We commit to forming strong community partnerships to enhance the trust of the citizens of Madison County. We believe community partnerships are critical elements of our organization. We commit to promoting teamwork and professional development and continually work to improve our professional performance. We believe that the prudent and effective management of our resources is critical to the future of our organization.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Table of Contents

Blank for Chief's Preface. 1

Law Enforcement Code of Ethics. 2

Blank for Mission Statement. 3

Chapter 1 - Law Enforcement Role and Authority. 10

100 - Law Enforcement Authority. 11
101 - Chief Executive Officer. 14
102 - Oath of Office. 15
103 - Policy Manual. 16
105 - Code of Ethics. 19

Chapter 2 - Organization and Administration. 20

200 - Organizational Structure and Responsibility. 21
201 - General Orders. 24
202 - Emergency Operations Plan. 25
203 - Training. 27
204 - Electronic Mail. 32
205 - Administrative Communications. 33
206 - Supervision Staffing Levels. 34
207 - Retired Officer Identification Card. 35

Chapter 3 - General Operations. 38

300 - Use of Force. 39
301 - Use of Force Review Boards. 48
302 - Handcuffing and Restraints. 51
303 - Control Devices. 56
304 - Conducted Energy Device. 61
305 - Officer-Involved Shootings and Deaths. 68
306 - Firearms. 77
307 - Vehicle Pursuits. 88
308 - Foot Pursuits. 101
309 - Deputy Response to Calls. 106
310 - Canines. 110
311 - Domestic or Family Violence. 120
312 - Search and Seizure. 127
313 - Child Abuse. 129
314 - Adult Abuse. 135
315 - Discriminatory Harassment. 140
316 - Missing Persons. 145
317 - Public Alerts. 153
318 - Victim and Witness Assistance. 158
319 - Hate Crimes. 162

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

320 - Standards of Conduct. 164
321 - Information Technology Use. 171
322 - Department Use of Social Media. 174
323 - Report Preparation. 177
324 - Media Relations. 182
325 - Subpoenas and Court Appearances. 185
326 - Part-Time Deputies. 187
327 - Auxiliary Positions. 191
328 - Outside Agency Assistance. 195
329 - Registered Offender Information. 197
330 - Major Incident Notification. 199
331 - Death Investigation. 201
332 - Private Person's Arrest. 204
333 - Limited English Proficiency Services. 205
334 - Communications with Persons with Disabilities. 213
335 - Mandatory Employer Notification. 221
336 - Biological Samples. 222
337 - Chaplains. 224
338 - Child and Dependent Adult Safety. 230
339 - Service Animals. 234
340 - Volunteers. 237
341 - Native American Graves Protection and Repatriation. 243
342 - Off-Duty Law Enforcement Actions. 245
343 - Human Trafficking. 247
344 - Community Relations. 251
345 - Substantial Risk Orders. 255
346 - School Resource Officers. 259

Chapter 4 - Patrol Operations. 262

400 - Patrol. 263
401 - Bias-Based Policing. 266
402 - Briefing. 269
403 - Crime and Disaster Scene Integrity. 271
404 - Crisis Response Unit. 273
405 - Ride-Alongs. 284
406 - Hazardous Material Response. 287
407 - Hostage and Barricade Incidents. 290
408 - Response to Bomb Calls. 295
409 - Crisis Intervention Incidents. 300
410 - Civil Commitments. 308
411 - Citation Releases. 312
412 - Foreign Diplomatic and Consular Representatives. 313
413 - Rapid Response and Deployment. 317
414 - Immigration Violations. 322
415 - Utility Service Emergencies. 325
416 - Aircraft Accidents. 327
417 - Field Training. 331

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

418 - Air Support. 335
419 - Contacts and Temporary Detentions. 336
420 - Criminal Organizations. 340
421 - Shift Supervisors. 344
422 - Mobile Audio/Video. 345
423 - Mobile Data Computer Use. 351
424 - Portable Audio/Video Recorders. 354
425 - Public Recording of Law Enforcement Activity. 358
426 - Automated License Plate Readers (ALPRs). 361
427 - Homeless Persons. 364
428 - Medical Marijuana. 367
429 - Medical Aid and Response. 369
430 - First Amendment Assemblies. 374
431 - Civil Disputes. 381
432 - Suspicious Activity Reporting. 384
433 - Procedures for Emergency and Temporary Custody Orders. 386
434 - Service of Court Documents. 388
435 - Court Security Policy. 392

Chapter 5 - Traffic Operations. 395

500 - Traffic. 396
501 - Traffic Accidents. 402
502 - Vehicle Towing. 406
503 - Vehicle Tow Hearings. 410
504 - Impaired Driving. 411
505 - Traffic and Parking Citations. 416
506 - Disabled Vehicles. 418
507 - Traffic Procedures. 420

Chapter 6 - Investigation Operations. 423

600 - Investigation and Prosecution. 424
601 - Sexual Assault Investigations. 430
602 - Asset Forfeiture. 435
603 - Informants. 441
604 - Eyewitness Identification. 447
605 - Brady Information. 451
606 - Unmanned Aerial System. 454
607 - Warrant Service. 457
608 - Operations Planning and Deconfliction. 461

Chapter 7 - Equipment. 466

700 - Department-Owned and Personal Property. 467
701 - Personal Communication Devices. 470
702 - Vehicle Maintenance. 474
703 - Vehicle Use. 477
704 - Fiscal Management. 484
705 - Personal Protective Equipment. 487

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Chapter 8 - Support Services. 492
800 - Crime Analysis. 493
801 - The Dispatch Center. 495
802 - Property and Evidence Section. 501
803 - Records Division. 511
804 - Records Maintenance and Release. 515
805 - Protected Information. 522
806 - Animal Control. 526
807 - Courthouse Security Operations. 530

Chapter 9 - Custody. 535
900 - Temporary Custody of Adults. 536
901 - Temporary Custody of Juveniles. 547
902 - Custodial Searches. 557
903 - Prison Rape Elimination. 562

Chapter 10 - Personnel. 572
1000 - Recruitment and Selection. 573
1001 - Performance Evaluations. 578
1002 - Special Assignments and Promotions. 582
1003 - Anti-Retaliation. 584
1004 - Reporting of Arrests, Convictions and Court Orders. 587
1005 - Drug- and Alcohol-Free Workplace. 589
1006 - Sick Leave. 592
1007 - Communicable Diseases. 594
1008 - Smoking and Tobacco Use. 599
1009 - Personnel Complaints. 600
1010 - Safety Belts. 609
1011 - Body Armor. 611
1012 - Personnel Records. 613
1013 - Request for Change of Assignment. 618
1014 - Commendations and Awards. 619
1015 - Fitness for Duty. 621
1016 - Meal Periods and Breaks. 624
1017 - Lactation Breaks. 625
1018 - Payroll Records. 627
1019 - Overtime Compensation. 628
1020 - Outside Employment and Outside Overtime. 630
1021 - Work-Related Disease, Injury, and Death Reporting. 635
1022 - Personal Appearance Standards. 637
1023 - Uniforms and Civilian Attire. 641
1024 - Conflict of Interest. 647
1025 - Badges, Patches, and Identification. 649
1026 - Temporary Modified-Duty Assignments. 652
1027 - Performance History Audits. 655
1028 - Speech, Expression and Social Networking. 658
1029 - Illness and Injury Prevention. 662

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1030 - Line-of-Duty Deaths. 667
1031 - Wellness Program. 678

Attachments. 683
605 IACP Brady-Giglio Training Outline.pdf. 684
Rappahannock Rapidan Transfer of Custody Form.pdf. 685
Detainee Personal Property Record Receipt.pdf. 686
Madison County Sexual Assault Response Team MOU (10-30-2020).pdf. 687
Ride-Along Application and Liability Waiver.pdf. 688
408 Bomb Threat Procedures and Checklist.pdf. 689
MCSO Instructions for Photo Array.pdf. 690
805 CJIS Security Policy Rev. 5.9.pdf. 691
Death Scene Checklist.pdf. 692
Naloxone Reporting Form.pdf. 693
SUPERVISORS REPORT OF EMPLOYEE ACCIDENT.pdf. 694
EMPLOYEE ACCIDENT REPORT.pdf. 695
Report of Discriminatory Harassment.pdf. 696
Employee and Supervisor Injury Report.pdf. 697
VA Madison County SO - Off Site Forensic Interview Protocol (2017).pdf. 698
Rappahannock Rapidan Community Services MOU.pdf. 699
Sample Lineup Case Information Sheet.pdf. 700
Rappahannock Rapidan MOU re Transfer of Custody.pdf. 701
406 USDOT HAZMAT Identification Guidebook.pdf. 702
Employee Performance Evaluation.pdf. 703
Workplace Safety Inspection Checklist.pdf. 704
Harrassment and Discrimination Acknowlegment.pdf. 705
Sergeant supplemental Eval.pdf. 706
604 Lineup Results Form.pdf. 707
604 Lineup Case Information Sheet.pdf. 708
1031 Workplace Accident Investigation Form.pdf. 709
FTO Form.pdf. 710
Employee Performance Evaluation 2.pdf. 711
CITAC Business Hours.pdf. 712
417 Field Training Program Completion Record and Competency Attestation.pdf. . . . 713
604 Eyewitness Lineup Instruction Form.pdf. 714
604 Eyewitness Sequential Photo Lineup Instruction Form.pdf. 715
604 Eyewitness Show-up Instruction Form.pdf. 716
ACCIDENT WITNESS STATEMENT.pdf. 717
VA Madison County SO - Victim Witness Agreement.pdf. 718
Madison County 2020 Co Nurse.pdf. 719
317 Virginia Senior Alert Plan - User Guide.pdf. 720
317 Virginia Senior Alert Request Form.pdf. 721
317 Virginia Missing Child With Autism Alert Plan User Guide.pdf. 722
334 I Speak Language Flashcards.pdf. 723
334 Language Identification Flash Cards.pdf. 724
MadiSon County School SRO MOU.pdf. 725
317 Virginia Senior Alert Termination Fax Form.pdf. 726

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

311 VA Summary of Crime Victim and Witness Rights Act.pdf. 727
Use of Force Report.pdf. 728
Citizen Complaint (Rev. March 2022).pdf. 729
200 VA Madison County Sheriffs Department Organizational Chart.pdf. 730
2020 Madison County - Basic Emergency Operations Plan.pdf. 731
Oath of Office.pdf. 732
MCSO LEOSA Waiver Form.pdf. 733
317 Virginia Missing Child with Autism Agency Termination Request Form.pdf. . . . 734
317 Virginia Missing Child with Autism Agency Activation Request Form.pdf. . . . 735
317 Virginia Ashanti Alert - Abducted Adult - Termination Fax Form.pdf. 736
317 Virginia Ashanti Alert - Abducted Adult - Activation Request Form.pdf. 737
317 Virginia Ashanti Alert - Abducted Adult - Plan.pdf. 738
317 Virginia AMBER Alert Plan (Rev. 3-1-21).pdf. 739
317 DOJ Amber Alert Field Guide for Law Enforcement Officers.pdf. 740
Threat Assessment Matrix .pdf. 741
VA Madison County Child Abuse Multi-Disciplinary Team (MDT Agreement July 1 2020.pdf. 742
316 HIPAA Compliant Medical Records Release Form.pdf. 743
316 Missing Child School Notification Form.pdf. 744
316 Investigative checklist for Missing Children.pdf. 745
316 Missing Persons Investigation Checklist.pdf. 746
SP-183_Va_Missing_Children_Info_Clearinghouse_Report.pdf. 747
SP-067_Va_Missing_Adult_Info_Clearinghouse_Report.pdf. 748
314 Checklist for Drug-Endangered Dependent Persons Investigations.pdf. 749
314 HIPAA Compliant Medical Records Release Form.pdf. 750
410 Statewide Standing Order for Nalaxone (1-14-2022).pdf. 751

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Chapter 1 - Law Enforcement Role and Authority

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Law Enforcement Authority

100.1 PURPOSE AND SCOPE

The purpose of this policy is to affirm the authority of the members of the Madison County Sheriff's Office to perform their functions based on established legal authority.

100.2 POLICY

It is the policy of the Madison County Sheriff's Office to limit its members to only exercise the authority granted to them by law.

While this department recognizes the power of peace officers to make arrests and take other enforcement action, deputies are encouraged to use sound discretion in the enforcement of the law. This department does not tolerate abuse of law enforcement authority.

100.3 LAW ENFORCEMENT OFFICER POWERS

Sworn members of this department are authorized to exercise law enforcement officer powers pursuant to applicable state law.

This includes authority for the prevention and detection of crime, the apprehension of criminals, the safeguard of life and property, the preservation of peace, and the enforcement of state and local laws, regulations, and ordinances (Va. Code § 15.2-1609; Va. Code § 15.2-1700; Va. Code § 15.2-1704; Va. Code § 52-8).

100.3.1 ARREST AUTHORITY WITHIN THE JURISDICTION OF THE MADISON COUNTY SHERIFF'S OFFICE

The arrest authority of deputies within the jurisdiction of the Madison County Sheriff's Office includes (Va. Code § 19.2-81):

(a) In compliance with an arrest warrant (Va. Code § 19.2-76).

(b) When any crime has been committed in the deputy's presence.

(c) When there is probable cause to believe that the offender has committed a felony.

(d) When there is probable cause to believe that the offender has committed:

  (a) A violation pertaining to the operation of a motor vehicle, watercraft, or motorboat while intoxicated and the arrest occurs within three hours of the offense.

  (b) A violation pertaining to the operation of a motor vehicle, watercraft, or motorboat while intoxicated and where an accident has occurred.

  (c) Misdemeanor shoplifting.

  (d) Misdemeanor carrying a weapon on school property.

  (e) Misdemeanor brandishing a firearm.

  (f) Misdemeanor destruction of a property located on premises used for business or commercial purposes.

  (g) Misdemeanor assault and battery.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(h) A violation of a protective order.

(i) A crime in another state which is punishable by imprisonment for a term exceeding one year (Va. Code § 19.2-100).

(e) When there is reasonable suspicion to believe that the individual has violated a criminal immigration law of the United States (Va. Code § 19.2-81.6).

(f) Violations involving quarantine or isolation orders related to communicable diseases (Va. Code § 15.2-1704; Va. Code § 32.1-48.014).

100.3.2 ARREST AUTHORITY OUTSIDE THE JURISDICTION OF THE MADISON COUNTY SHERIFF'S OFFICE

The arrest authority of deputies outside the jurisdiction of the Madison County Sheriff's Office includes:

(a) When there is probable cause to arrest a person who has escaped or who has fled to avoid arrest and the deputy has been in continuous close pursuit from within the jurisdiction of the Madison County Sheriff's Office (Va. Code § 19.2-77).

(b) When another agency has requested temporary assistance during an emergency declared by the chief law enforcement officer of that agency (Va. Code § 15.2-1730).

Whenever a deputy makes an arrest outside the department's jurisdiction, the deputy should, as soon as practicable, either take the arrested person before a judicial officer in the locality where the arrest was made or transfer custody of the person to the proper law enforcement authority with jurisdiction in the locality (Va. Code § 19.2-76).

100.3.3 GRANTING AUTHORITY TO OTHERS

Deputies may require the assistance of any person to arrest another for any breach of the peace or to capture another who has escaped from custody (Va. Code § 18.2-463).

100.3.4 PROHIBITION OF QUOTAS

This department does not establish arrest or summons quotas. The number of arrests made or summons issued by any member shall not be used as the sole criterion for evaluating member overall performance (Va. Code § 2.2-5516; Va. Code § 15.2-1609.11; Va. Code § 15.2-1710.1).

100.4 INTERSTATE LAW ENFORCEMENT AUTHORITY

Law enforcement authority may be extended to other states:

(a) As applicable under interstate compacts, memorandums of understanding, or mutual aid agreements in compliance with the laws of each state.

(b) When a deputy enters the following states while in pursuit of a person who the deputy has probable cause to believe has committed a felony:

1. The District of Columbia (D.C. Code § 23-901)
2. Maryland (Md. Code CP § 2-305)
3. Tennessee (T.C.A. § 40-7-203)

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

4. West Virginia (W. Va. Code § 62-11-1)

(c) When a deputy enters North Carolina while in pursuit of a person who the pursuing deputy has probable cause to believe has committed a criminal offense (N.C.G.S. § 15A-403).

Whenever a deputy makes an arrest in the District of Columbia, Maryland, Tennessee, West Virginia, or North Carolina the deputy shall take the offender to a magistrate or judge in the county where the arrest occurred as soon as practicable (D.C. Code § 23-902; Md. Code CP § 2-306; T.C.A. § 40-7-204; W. Va. Code § 62-11-2; N.C.G.S. § 15A-403).

100.5 CONSTITUTIONAL REQUIREMENTS

All members shall observe and comply with every person’s clearly established rights under the United States and Virginia constitutions.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Chief Executive Officer

101.1 PURPOSE AND SCOPE

All law enforcement Chief Executive Officers employed within the Commonwealth of Virginia are required to meet specific requirements for appointment. This policy provides guidelines for the appointment of the Chief Executive Officer of the Madison County Sheriff's Office, who is required to exercise the powers and duties of the office as prescribed by law (Va. Code § 15.2-1701; Va. Code § 15.2-1609).

101.2 POLICY

It is the policy of the Madison County Sheriff's Office that the Sheriff meets the minimum standards for exercising his/her authority granted by law.

101.3 SHERIFF REQUIREMENTS

The Sheriff of this department, as a condition of continued employment, shall be:

(a) Qualified to vote for and hold the office sought (Va. Code § 24.2-500).

(b) A resident of the Commonwealth for one year immediately preceding the election.

(c) Elected by the qualified voters of the county (Va. Const. art. VII, § 4; Va. Code § 15.2-1609).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Oath of Office

102.1 PURPOSE AND SCOPE

The purpose of this policy is to ensure that oaths, when appropriate, are administered to department members.

102.2 POLICY

It is the policy of the Madison County Sheriff's Office that, when appropriate, department members affirm the oath of their office as an expression of commitment to the constitutional rights of those served by the Department and the dedication of its members to their duties.

102.3 OATH OF OFFICE

All department members, upon assuming sworn status, shall take and subscribe before a magistrate, a notary, a commissioner in chancery, a commissioner appointed by the Governor, a judge or clerk or deputy clerk of court, a commissioner or clerk or deputy clerk of the State Corporation Commission, or clerks of governing bodies of local governments, to the following oaths or affirmations applicable to the member's position (Va. Code § 49-4; Va. Code § 49-1).

The form of the oath shall be as follows:

"I, (employee name), do solemnly swear (or affirm) that I will support the Constitution of the United States, and the Constitution of the Commonwealth of Virginia, and that I will faithfully and impartially discharge all the duties incumbent upon me as (the/a/an title or position) according to the best of my ability, (so help me God)."

If a member is opposed to taking an oath, the member shall be permitted to substitute the word "affirm" for the word "swear," and the words "so help me God" shall be omitted.

102.4 MAINTENANCE OF RECORDS

The oath of office shall be filed as prescribed by law (Va. Code § 49-8).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Policy Manual

103.1 PURPOSE AND SCOPE

The manual of the Madison County Sheriff's Office is hereby established and shall be referred to as the Policy Manual or the manual. The manual is a statement of the current policies, procedures, rules and guidelines of this department. All members are to conform to the provisions of this manual.

All prior and existing manuals, orders and regulations that are in conflict with this manual are rescinded, except to the extent that portions of existing manuals, orders and other regulations that have not been included herein shall remain in effect where they do not conflict with the provisions of this manual.

103.2 POLICY

Except where otherwise expressly stated, the provisions of this manual shall be considered as guidelines. It is recognized that the work of law enforcement is not always predictable and that circumstances may arise that warrant departure from these guidelines. It is the intent of this manual to be viewed from an objective standard, taking into consideration the sound discretion entrusted to members of this department under the circumstances reasonably available at the time of any incident.

103.2.1 DISCLAIMER

The provisions contained in the Policy Manual are not intended to create an employment contract nor any employment rights or entitlements. The policies contained within this manual are for the internal use of the Madison County Sheriff's Office and shall not be construed to create a higher standard or duty of care for civil or criminal liability against the County, its officials or department members. Violations of any provision of any policy contained within this manual shall only form the basis for administrative action, training or discipline. The Madison County Sheriff's Office reserves the right to revise any policy content, in whole or in part.

103.3 AUTHORITY

The Sheriff shall be considered the ultimate authority for the content and adoption of the provisions of this manual and shall ensure compliance with all applicable federal, state and local laws. The Sheriff or the authorized designee is authorized to issue General Orders, which shall modify those provisions of the manual to which they pertain. General Orders shall remain in effect until such time as they may be permanently incorporated into the manual.

103.4 DEFINITIONS

The following words and terms shall have these assigned meanings throughout the Policy Manual, unless it is apparent from the content that they have a different meaning:

Adult - Any person 18 years of age or older (Va. Code § 1-203).

County - The County of Madison County, Virginia.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Policy Manual

Non-sworn - Employees and volunteers who are not sworn law enforcement officers.

Department/MCSO - The Madison County Sheriff's Office.

Employee - Any person employed by the Department.

Manual - The Madison County Sheriff's Office Policy Manual.

May - Indicates a permissive, discretionary or conditional action.

Member - Any person who is appointed to or employed by the Madison County Sheriff's Office, including:

- Full- or part-time employees
- Sworn deputies
- Reserve, auxiliary deputies
- Non-sworn employees
- Volunteers

Deputy - Those employees, regardless of rank, who are sworn law enforcement employees of the Madison County Sheriff's Office (Va. Code § 9.1-101).

On-duty - A member’s status during the period when he/she is actually engaged in the performance of his/her assigned duties.

Order - A written or verbal instruction issued by a superior.

Rank - The title of the classification held by a deputy.

Shall or will - Indicates a mandatory action.

Should - Indicates a generally required or expected action, absent a rational basis for failing to conform.

Supervisor - A person in a position of authority regarding hiring, transfer, suspension, promotion, discharge, assignment, reward or discipline of other department members, directing the work of other members or having the authority to adjust grievances. The supervisory exercise of authority may not be merely routine or clerical in nature but requires the use of independent judgment.

The term "supervisor" may also include any person (e.g., deputy-in-charge, lead or senior worker) given responsibility for the direction of the work of others without regard to a formal job title, rank or compensation.

When there is only one department member on-duty, that person may also be the supervisor, except when circumstances reasonably require the notification or involvement of the member’s off-duty supervisor or an on-call supervisor.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Policy Manual

103.5 ISSUING THE POLICY MANUAL

An electronic version of the Policy Manual will be made available to all members on the department network for viewing and printing. No changes shall be made to the manual without authorization from the Sheriff or the authorized designee.

Each member shall acknowledge that he/she has been provided access to and has had the opportunity to review the Policy Manual and General Orders. Members shall seek clarification as needed from an appropriate supervisor for any provisions that they do not fully understand.

103.6 PERIODIC REVIEW OF THE POLICY MANUAL

The Sheriff will ensure that the Policy Manual is periodically reviewed and updated as necessary.

103.7 REVISIONS TO POLICIES

All revisions to the Policy Manual will be provided to each member on or before the date the policy becomes effective. Each member will be required to acknowledge that he/she has reviewed the revisions and shall seek clarification from an appropriate supervisor as needed.

Members are responsible for keeping abreast of all Policy Manual revisions.

Each Division Supervisor will ensure that members under his/her command are aware of any Policy Manual revision.

All department members suggesting revision of the contents of the Policy Manual shall forward their written suggestions to their Division Supervisors, who will consider the recommendations and forward them to the command staff as appropriate.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Code of Ethics

105.1 PURPOSE AND SCOPE

The purpose of this policy is to ensure that all members are aware of their individual responsibilities to maintain their integrity and that of their department at all times.

105.2 POLICY

The Law Enforcement Code of Ethics shall be received and abided by all deputies of the Department.

105.3 LAW ENFORCEMENT CODE OF ETHICS

Sworn members shall abide by the following Code of Ethics:

AS A LAW ENFORCEMENT OFFICER, my fundamental duty is to serve the community; to safeguard lives and property; to protect the innocent against deception, the weak against oppression or intimidation, and the peaceful against abuse or disorder; and to respect the constitutional rights of all to liberty, equality, and justice.

I will keep my private life unsullied as an example to all and will behave in a manner that does not bring discredit to me or to my agency. I will maintain courageous calm in the face of danger, scorn, or ridicule; develop self-restraint; and be constantly mindful of the welfare of others. Honest in thought and deed both in my personal and official life, I will be exemplary in obeying the law and the regulations of my department. Whatever I see or hear of a confidential nature or that is confided to me in my official capacity will be kept ever secret unless revelation is necessary in the performance of my duty.

I will never act officiously or permit personal feelings, prejudices, political beliefs, aspirations, animosities, or friendships to influence my decisions. With no compromise for crime and with relentless prosecution of criminals, I will enforce the law courteously and appropriately without fear or favor, malice or ill will, never employing unnecessary force or abuse, and never accepting gratuities.

I recognize the badge of my office as a symbol of public faith, and I accept it as a public trust to be held so long as I am true to the ethics of police service. I will never engage in acts of corruption or bribery, nor will I condone such acts by other police officers. I will cooperate with all legally authorized agencies and their representatives in the pursuit of justice.

I know that I alone am responsible for my own standard of professional performance and will take every reasonable opportunity to enhance and improve my level of knowledge and competence.

I will constantly strive to achieve these objectives and ideals, dedicating myself before God to my chosen profession...law enforcement.

105.3.1 OBJECTION TO RELIGIOUS AFFIRMATION

Reference to religious affirmation in the Law Enforcement Code of Ethics may be omitted where objected to by the deputy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Chapter 2 - Organization and Administration

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Organizational Structure and Responsibility

200.1 PURPOSE AND SCOPE

This policy establishes the organizational structure of the Department and defines general responsibilities of department members.

200.2 POLICY

The Madison County Sheriff's Office will implement and maintain an organizational structure that provides clear and identifiable roles for command, control and guidance of the Department. Each position and assignment has clearly identified responsibilities and a defined chain of command.

See attachment: 200 VA Madison County Sheriffs Department Organizational Chart.pdf

200.3 DIVISIONS

The Sheriff is responsible for administering and managing the Madison County Sheriff's Office. The Captain shall oversee the administration and operations of the Patrol and Investigation Divisions, and of the Crisis Response Unit. There are three divisions in the Department:

- Administration Division
- Patrol Division
- Investigation Division

200.3.1 ADMINISTRATION DIVISION

The Administration Division is commanded by the Sheriff, whose primary responsibility is to provide general management, direction, and control for the Administration Division. The Administration Division consists of technical and administrative services including the Sheriff's Administrative Assistant and Records Management Section. The Administration Division also includes the Property and Evidence Section which is commanded by the Major.

200.3.2 PATROL DIVISION

The Patrol Division is commanded by a Lieutenant, whose primary responsibility is to provide general management, direction and control for the Patrol Division. The Patrol Division consists of uniformed patrol and special operations, which includes the Patrol Division and the Court Services Unit.

200.3.3 INVESTIGATION DIVISION

The Investigation Division is commanded by a Lieutenant, whose primary responsibility is to provide general management, direction, and control for the Investigation Division. The Investigation Division consists of the Investigation Division, crime analysis and forensic services, and the School resources Officers.

200.4 COMMAND PROTOCOL

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Organizational Structure and Responsibility

200.4.1 SUCCESSION OF COMMAND
The Sheriff exercises command over all members of the Madison County Sheriff's Office. During planned absences, the Sheriff will designate a Division Supervisor to serve as the acting Sheriff or perform the executive command function.

Except when designated as above, the order of command authority in the absence or unavailability of the Sheriff is as follows:

(a) Patrol Division Supervisor

(b) Investigation Division Supervisor

(c) Administration Division Supervisor

(d) On-duty Shift Supervisor

200.4.2 UNITY OF COMMAND
The principles of unity of command ensure efficient supervision and control within the Department. Generally, each member shall be accountable to one supervisor at any time for a given assignment or responsibility. Each organizational component of the department is under the direct command of one supervisor. Supervisors are accountable for employees under their immediate supervision. Except where specifically delegated authority may exist by policy or special assignment (e.g., Canine, Bicycle Patrol), any supervisor may temporarily direct any subordinate if an operational necessity exists. Members should proceed directly up the chain of command for resolution should they believe that they received conflicting or unlawful orders.

200.5 AUTHORITY AND RESPONSIBILITIES
Each member will be assigned duties and responsibilities. Each member is delegated the authority necessary to effectively execute those responsibilities. Each member will also be held accountable for the appropriate application of that delegated authority.

200.6 OPERATIONAL AUDITS
Division Supervisors are responsible for ensuring that line inspections and staff evaluations are conducted for reviewing and evaluating the operations of programs under their command. The focus of the inspections should include adherence to the Department's goals and mission statement, policies and procedures, and performance targets, as well as adequacy of resources and staffing or other subject matter as directed by the Sheriff or the authorized designee.

(a) Line inspections should be conducted at least monthly by personnel who supervise the program being inspected and include:

1. Announced or unannounced inspections of facilities, equipment, uniforms, procedures, and performance capabilities.
2. An assessment of compliance with the program's goals, mission, policies and procedures, and target performance levels.
3. A written report noting any serious or recurring deficiencies.
4. A written plan to correct any identified deficiencies.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Staff evaluations should be conducted at least every three years at the direction of the Sheriff by personnel who do not directly supervise the program being inspected and include:

1. Announced formal evaluations of facilities, equipment, uniforms, procedures, and performance capabilities.
2. An assessment of compliance with the program's goals, mission, policies and procedures, and target performance levels.
3. A written report of the program's performance level, including notation of any serious or recurring deficiencies.
4. A written plan to correct any identified deficiencies.

Summary reports of staff evaluations and line inspections shall be forwarded through the chain of command to the Sheriff or the authorized designee.

200.7 DEPARTMENT GOALS AND OBJECTIVES

The Sheriff or the authorized designee should establish goals and objectives for the Madison County Sheriff's Office. The plan should specify a time period and should include, but is not limited to:

- Long-term goals and operational objectives.
- Anticipated workload and staffing needs.
- Capital improvement, equipment and supply needs.
- Provisions for implementation, progress assessment and revision as needed.

Goals and objectives should be reviewed annually by the Sheriff or the authorized designee and updated as required.

Division Supervisors are responsible for the planning and research function. This function is essential to effective agency management and includes careful research of operational alternatives and the planning of future programs.Division Supervisors should ensure that goals and objectives for their assigned Divisions are established, assessed for progress, reviewed and updated annually, and distributed to all affected members.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

General Orders

201.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for issuing General Orders.

201.2 POLICY

General Orders will be used to modify policies of the Madison County Sheriff's Office when an immediate need to adapt a policy or procedure exists, in order to best meet the mission of the Department. Applicable law, County policy and rules should be considered before a General Order is issued.

201.3 PROTOCOL

General Orders will be incorporated into the Policy Manual, as required, upon approval. General Orders will modify existing policies or create a new policy as appropriate and will be rescinded if incorporated into the Policy Manual.

The Sheriff or the authorized designee should ensure that all General Orders are disseminated appropriately. General Orders should be numbered consecutively and incorporate the year of issue. All members will be notified when a General Order is rescinded or has been formally adopted into the Policy Manual.

201.4 RESPONSIBILITIES

201.4.1 COMMAND STAFF

Command staff shall periodically review General Orders to determine whether they should be formally incorporated into the Policy Manual and, as appropriate, will recommend necessary modifications to the Sheriff.

201.4.2 SHERIFF

Only the Sheriff or the authorized designee may approve and issue General Orders.

201.5 ACCEPTANCE OF DIRECTIVES

All members shall be provided access to the General Orders. Each member shall acknowledge that he/she has been provided access to and has had the opportunity to review the General Orders. Members shall seek clarification as needed from an appropriate supervisor for any provisions they do not fully understand.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Emergency Operations Plan

202.1 PURPOSE AND SCOPE

This policy clarifies the role of the Madison County Sheriff's Office and responsibilities of its members pertaining to large scale emergencies and the Commonwealth of Virginia Emergency Operations Plan.

202.2 POLICY

The Madison County Sheriff's Office will prepare for large-scale emergencies within and outside its jurisdiction through planning and mutual cooperation with other agencies (Va. Code § 44-146.19).

The County Emergency Operations Plan complies with the Commonwealth of Virginia's Emergency Operation Plan. This plan provides guidance for County emergency operations within and outside its borders as may be required.

See attachment: 2020 Madison County - Basic Emergency Operations Plan.pdf

202.2.1 MADISON COUNTY, VIRGINIA CODES/ORDINANCES

An emergency management organization has been established by the County of Madison County, Virginia. This ordinance has been approved by the Board of Supervisors (Va. Code § 44-146.19).

202.3 DEPARTMENT RESPONSIBILITIES

The Department shall execute and enforce the orders, rules and regulations issued pursuant to the Emergency Operations Plan (Va. Code § 44-146.26).

202.4 ACTIVATING THE EMERGENCY OPERATIONS PLAN

The Emergency Operations Plan can be activated in a number of ways. For the Madison County Sheriff's Office, the Sheriff or the highest ranking on-duty supervisor may activate the Emergency Operations Plan in response to a major emergency.

Upon activation of the plan, the Sheriff or the authorized designee should contact the Virginia Department of Emergency Management (VDEM) to assist with mutual aid response from local, state and federal law enforcement agencies.

202.4.1 RECALL OF PERSONNEL

In the event that the Emergency Operations Plan is activated, all employees of the Madison County Sheriff's Office are subject to immediate recall to service. Employees may also be subject to recall during extraordinary circumstances as deemed necessary by the Sheriff or the highest ranking on-duty supervisor.

Failure to promptly respond to an order to report for duty may result in discipline.

202.5 LOCATION OF THE EMERGENCY OPERATIONS PLAN

Copies of the Emergency Operations Plan are available in Administration, the Shift Supervisor's office and the Dispatch Center. All supervisors should familiarize themselves with the Emergency Operations Plan and the roles members will play when the plan is implemented. The Sheriff

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

should ensure that department members are familiar with the roles they will play when the plan is implemented.

202.6 EMERGENCY OPERATIONS PLAN ASSESSMENT

The Sheriff or the authorized designee should complete an assessment of the Emergency Operations Plan at least once each year and ensure that the plan conforms to any revisions made by the National Incident Management System (NIMS) and VDEM. The Sheriff or the authorized designee should appropriately address any needed revisions (Va. Code § 44-146.18).

202.7 TRAINING

The Department should provide annual training on the Emergency Operations Plan for all supervisors and other appropriate personnel. All supervisors should familiarize themselves with the Emergency Operations Plan and personnel responsibilities when the plan is implemented. Training should incorporate a full or partial exercise, tabletop or command discussion.

The Department should participate in any statewide emergency response drills as requested by the Governor of Virginia (Va. Code § 44-146.17:2).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Training

203.1 PURPOSE AND SCOPE

This policy establishes general guidelines for how training is to be identified, conducted and documented. This policy is not meant to address all specific training endeavors or identify every required training topic.

203.2 POLICY

The Department shall administer a training program that will meet the standards of federal, state, local and the Virginia Department of Criminal Justice Services (DCJS) training requirements. It is a priority of this department to provide continuing education and training for the professional growth and development of its members.

203.3 OBJECTIVES

The objectives of the training program are to:

(a) Ensure that training is based on a curriculum that includes the most frequent assignments and tasks of law enforcement activities and that appropriate evaluation techniques are used to measure competency of required skills, knowledge and abilities.

(b) Enhance the level of law enforcement service to the public.

(c) Increase the technical expertise and overall effectiveness of department members.

(d) Provide for continued professional development of department members.

(e) Ensure compliance with DCJS rules and regulations concerning law enforcement training.

203.4 TRAINING SUPERVISOR

The Sheriff shall designate a Training Supervisor who is responsible for developing, reviewing, updating, and maintaining the department training plan so that required training is completed. The Training Supervisor should review the training plan annually.

203.4.1 TRAINING SUPERVISOR RESPONSIBILITIES

The Training Supervisor shall provide the DCJS with verification that members have met minimum standards set forth in Va. Code § 15.2-1705 (Va. Code § 15.2-1706).

203.5 TRAINING PLAN

The training plan should include the anticipated costs associated with each type of training, including attendee salaries and backfill costs. The plan should include a systematic and detailed method for recording and logging of all training for all members.

While updates and revisions may be made to any portion of the training plan at any time it is deemed necessary, the Training Supervisor shall review the entire training plan on an annual basis.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Training

The plan will include information on curriculum, training material, training facilities, and scheduling. The plan will address federal, state, and department-required, minimum-mandated training of deputies and other members.

203.5.1 GOVERNMENT-MANDATED TRAINING

The following lists, while not all inclusive, identify training that is required under state and federal laws and regulations. Additional required training may be identified in individual policies.

(a) Federally mandated training:
    1. National Incident Management System (NIMS) training

(b) State-mandated training for deputies requires completion of (Va. Code § 9.1-102):
    1. No less than 480 hours of academy training, within one year of their appointment, in the following areas (6 VAC 20-20-21; 6 VAC 20-20-40):
        (a) Professionalism
        (b) Legal
        (c) Communication
        (d) Patrol
        (e) Investigations
        (f) Defensive tactics and use of force
        (g) Weapons
        (h) Driver training
    2. No less than 240 hours of field training within one year of their appointment (6 VAC 20-20-21; 6 VAC 20-20-40).
    3. No less than 40 hours of in-service training biennially. Training shall consist of (6 VAC 20-30-30):
        (a) Two hours of cultural diversity training.
        (b) Four hours of legal training, which shall include training on new laws and revisions to existing laws that affect the department's responsibilities.
        (c) 34 hours of career development/elective training.
    4. Annual in-service training must be completed by December 31 of the calendar year (6 VAC 20-30-40).
    5. Annual DCJS-approved firearms training and qualification (6 VAC 20-30-80).

203.5.2 POSITIONS REQUIRING SPECIALIZED TRAINING

Deputies assigned to the following positions shall receive specialized training before performing the assignment, and in-service training as required for the position:

(a) Crisis Response Unit member (see the Crisis Response Unit Policy)

(b) Investigator

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) Motorcycle deputy

(d) Bicycle Patrol deputy (see the Bicycle Patrol Policy)

(e) Canine handler (see the Canines Policy)

(f) Traffic Crash Reconstructionist

(g) Field Training Officer (see the Field Training Policy)

(h) Community Relations/Training Officer (see the Community Relations Policy)

(i) School Resource Officer and/or Drug Abuse Resistance Education (D.A.R.E.) deputy

(j) Court officer

203.6 TRAINING COMMITTEE

The Training Supervisor may establish a Training Committee, on a temporary or as-needed basis, which will assist with identifying training needs.

The Training Committee should be composed of at least three members, with the senior ranking member of the committee acting as the chairperson. Committee members should be selected based on their abilities at post-incident evaluation and at assessing related training needs. The Training Supervisor may remove or replace members of the committee at his/her discretion.

The Training Committee should review certain incidents to determine whether training would likely improve future outcomes or reduce or prevent the recurrence of the undesirable issues related to an incident. Specific incidents the Training Committee should review include but are not limited to:

(a) Any incident involving the death or serious injury of a member.

(b) Incidents involving a high risk of death, serious injury, or civil liability.

(c) Incidents identified by the Department to determine possible training needs.

The Training Committee should convene on a regular basis, as determined by the Training Supervisor, to review the identified incidents. The committee shall determine by consensus whether a training need exists and then submit written recommendations of its findings to the Training Supervisor. The recommendation should not identify specific facts of any incidents, such as identities of members involved or the date, time, and location of the incident, but should focus on the type of training being recommended.

The Training Supervisor will consider the recommendations of the committee and determine what training should be addressed, taking into consideration the mission of the Department and the available resources. Training recommendations as determined by the Training Supervisor shall be submitted to the command staff for review.

203.7 TRAINING ATTENDANCE

(a) All members assigned to attend training shall attend as scheduled unless previously excused by their immediate supervisor. Excused absences should be limited to:

1. Court appearances.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. Previously approved vacation or time off.
3. Illness or medical leave.
4. Physical limitations preventing the member's participation.
5. Emergency situations or department necessity.

(b) Any member who is unable to attend training as scheduled shall notify his/her supervisor as soon as practicable but no later than two hours prior to the start of training and shall:

1. Document his/her absence in a memorandum to his/her supervisor.
2. Make arrangements through his/her supervisor or the Training Supervisor to attend the required training on an alternate date.

203.8 DAILY TRAINING BULLETINS

The Lexipol Daily Training Bulletins (DTBs) are contained in a web-accessed system that provides training on the Madison County Sheriff's Office Policy Manual and other important topics. Generally, one training bulletin is available for each day of the month. However, the number of DTBs may be adjusted by the Training Supervisor.

Members assigned to participate in DTBs shall only use the login credentials assigned to them by the Training Supervisor. Members should not share their password with others and should frequently change their password to protect the security of the system. After each session, members should log off the system to prevent unauthorized access. The content of the DTBs is copyrighted material and shall not be shared with others outside of the Department.

Members who are assigned to participate in the DTB program should complete each DTB at the beginning of their shifts or as otherwise directed by their supervisor. Members should not allow uncompleted DTBs to build up over time, and may be required to complete DTBs missed during extended absences (e.g., vacation, medical leave) upon returning to duty. Although the DTB system can be accessed from any internet-enabled computer, members shall only take DTBs as part of their on-duty assignments, unless directed otherwise by a supervisor.

Supervisors will be responsible for monitoring the progress of those under their command to ensure compliance with this policy.

203.9 TRAINING RECORDS

The Training Supervisor is responsible for the creation, filing and storage of all training records to include the type of training, dates/hours attended, instructor/location and members attending. Training records shall be retained in accordance with the established records retention schedule.

203.10 NON-SWORN ORIENTATION

The Training Supervisor or the authorized designee should provide all newly-appointed non-sworn members with information regarding the following:

(a) The Department's role, purpose, goals, policies, and procedures

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Working conditions and regulations

(c) Responsibilities and rights of members

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Electronic Mail

204.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the proper use and application of the electronic mail (email) system provided by the Department.

204.2 POLICY

Madison County Sheriff's Office members shall use email in a professional manner in accordance with this policy and current law (e.g., The Virginia Freedom of Information Act).

204.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to emails accessed, transmitted, received or reviewed on any department technology system (see the Information Technology Use Policy for additional guidance).

204.4 RESTRICTIONS ON USE OF EMAIL

Messages transmitted over the email system are restricted to official business activities, or shall only contain information that is essential for the accomplishment of business-related tasks or for communications that are directly related to the business, administration or practices of the Department.

Sending derogatory, defamatory, obscene, disrespectful, sexually suggestive, harassing or any other inappropriate messages on the email system is prohibited and may result in discipline.

Email messages addressed to the entire Department are only to be used for official business-related items that are of particular interest to all users. In the event that a member has questions about sending a particular email communication, the member should seek prior approval from a supervisor in his/her chain of command.

It is a violation of this policy to transmit a message under another member's name or email address or to use the password of another to log into the system unless directed to do so by a supervisor. Members are required to log off the network or secure the workstation when the computer is unattended. This added security measure will minimize the potential misuse of a member's email, name or password. Any member who believes his/her password has become known to another person shall change their password immediately.

204.5 EMAIL RECORD MANAGEMENT

Email may, depending upon the individual content, be a public record under the Virginia Freedom of Information Act and must be managed in accordance with the established records retention schedule and in compliance with state law.

The Custodian of Records shall ensure that email messages are retained and recoverable as outlined in the Records Maintenance and Release Policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Administrative Communications

205.1 PURPOSE AND SCOPE

This policy sets forth the manner in which the Department communicates significant changes to its membership, such as promotions, transfers, hiring and appointment of new members, separations, individual and group awards and commendations, or other changes in status. This policy also provides guidelines for the professional handling of electronic and non-electronic administrative communications from the Department.

205.2 POLICY

The Madison County Sheriff's Office will appropriately communicate significant events within the organization to its members. Both electronic and non-electronic administrative communications will be professional in appearance and comply with the established letterhead, signature and disclaimer guidelines, as applicable.

205.3 MEMORANDUMS

Memorandums may be issued periodically by the Sheriff or the authorized designee to announce and document all promotions, transfers, hiring and appointment of new members, separations, individual and group awards and commendations, or other changes in status.

205.4 CORRESPONDENCE

To ensure that the letterhead and name of the Department are not misused, all official external correspondence shall be on department letterhead. All department letterhead shall bear the signature element of the Sheriff. Official correspondence and use of letterhead requires approval of a supervisor. Department letterhead may not be used for personal purposes.

Official internal correspondence shall be on the appropriate department electronic or non-electronic memorandum forms.

Electronic correspondence shall contain the sender's department-approved signature and electronic communications disclaimer language.

205.5 SURVEYS

All surveys made in the name of the Department shall be authorized by the Sheriff or the authorized designee.

205.6 OTHER COMMUNICATIONS

General Orders and other communications necessary to ensure the effective operation of the Department shall be issued by the Sheriff or the authorized designee (see the General Orders Policy).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Supervision Staffing Levels

206.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines to ensure that proper supervision is available to meet the needs of the Department and members throughout all Divisions.

206.2 POLICY

The Madison County Sheriff's Office will ensure that proper supervision is available to meet the needs of its members and to achieve the goals of the Department. The needs of its members should be balanced with the needs of the Department for flexibility and discretion in assigning members to meet supervisory needs. While balance is desirable, the paramount concern is to meet the needs of the Department.

206.3 MINIMUM SUPERVISION STAFFING LEVELS

Minimum staffing levels should be established by the Division Supervisors for each Division and work group. The supervision staffing levels should support proper supervision, span of control, compliance with any County rule or policy, and activity levels to meet the needs of members and the goals of the Department.

206.3.1 TEMPORARY SUPERVISORS

In order to accommodate training and other unforeseen circumstances, a qualified lower-ranking member may be used as a temporary supervisor in place of a regularly assigned supervisor.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Retired Officer Identification Card

207.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the issuance, denial, suspension or revocation of Madison County Sheriff's Office identification cards to qualified former or retired law enforcement officers under the Law Enforcement Officers' Safety Act (LEOSA) and Virginia law (18 USC § 926C; Va. Code § 9.1-1000).

207.2 POLICY

It is the policy of the Madison County Sheriff's Office to provide identification cards to qualified former or retired deputies to facilitate the lawful carrying of concealed weapons by those individuals.

207.3 LEOSA

The Sheriff may issue an identification card for LEOSA purposes to any qualified former deputy of this department who (18 USC § 926C(c)):

(a) Separated from service in good standing from this department as a deputy.

(b) Before such separation, had regular employment as a law enforcement officer for an aggregate of 10 years or more or, if employed as a law enforcement officer for less than 10 years, separated from service after completing any applicable probationary period due to a service-connected disability as determined by this department.

(c) Has not been disqualified for reasons related to mental health.

(d) Has not entered into an agreement with this department where the deputy acknowledges that he/she is not qualified to receive a firearms qualification certificate for reasons related to mental health.

(e) Is not prohibited by federal law from receiving or possessing a firearm.

207.3.1 LEOSA CARD FORMAT

The LEOSA identification card should contain a photograph of the former deputy and identify him/her as having been employed as a deputy.

If the Madison County Sheriff's Office qualifies the former deputy, the LEOSA identification card or separate certification should indicate the date the former deputy was tested or otherwise found by the Department to meet the active-duty standards for qualification to carry a firearm.

207.3.2 AUTHORIZATION

Any qualified former law enforcement officer, including a former deputy of this department, may carry a concealed firearm under 18 USC § 926C when he/she is:

(a) In possession of photographic identification that identifies him/her as having been employed as a law enforcement officer, and one of the following:

1. An indication from the person's former law enforcement agency that he/she has, within the past year, been tested or otherwise found by the law enforcement

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

agency to meet agency-established active-duty standards for qualification in firearms training to carry a firearm of the same type as the concealed firearm.

2. A certification, issued by either the state in which the person resides or by a certified firearms instructor who is qualified to conduct a firearms qualification test for active-duty law enforcement officers within that state, indicating that the person has, within the past year, been tested or otherwise found to meet the standards established by the state or, if not applicable, the standards of any agency in that state.

(b) Not under the influence of alcohol or another intoxicating or hallucinatory drug or substance.

(c) Not prohibited by federal law from receiving a firearm.

(d) Not in a location prohibited by Virginia law or by a private person or entity on his/her property if such prohibition is permitted by Virginia law.

207.4 RETIRED OFFICER IDENTIFICATION CARD

The Sheriff shall issue a retired officer identification card, upon request, to a deputy who has retired from this department as a law enforcement officer. In certain circumstances, this card is required to be issued in a format that prevents it from being carried on the person (Va. Code § 9.1-1000).

The retired officer identification card shall include an endorsement to carry a concealed firearm if the retired deputy has met the requirements of Va. Code § 18.2-308.016.

If the Department qualifies the retiree, the card may include the date that the retiree was qualified by the Department to carry a firearm in compliance with 18 USC § 926C(d)(1).

207.4.1 AUTHORIZATION

Qualified former deputies with a retired officer identification card issued by the Department under state law may carry concealed, within this state, any firearm inspected and approved by the Department. The card does not itself authorize a retiree to carry a concealed firearm outside this state. The former deputy must also meet state and LEOSA requirements (Va. Code § 18.2-308.014).

207.5 FORMER DEPUTY RESPONSIBILITIES

A former deputy with a card issued under this policy shall immediately notify the Shift Supervisor of his/her arrest or conviction in any jurisdiction, or that he/she is the subject of a court order, in accordance with the Reporting of Arrests, Convictions and Court Orders Policy.

207.5.1 RESPONSIBILITIES UNDER LEOSA

In order to obtain or retain a LEOSA identification card, the former deputy shall:

(a) Sign a waiver of liability of the Department for all acts taken related to carrying a concealed firearm, acknowledging both his/her personal responsibility as a private person for all acts taken when carrying a concealed firearm as permitted by LEOSA and also that these acts were not taken as an employee or former employee of the Department.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Remain subject to all applicable department policies and federal, state and local laws.

(c) Demonstrate good judgment and character commensurate with carrying a loaded and concealed firearm.

(d) Successfully pass an annual criminal history background check indicating that he/she is not prohibited by law from receiving or possessing a firearm.

See attachment: MCSO LEOSA Waiver Form.pdf

207.5.2 RESPONSIBILITIES UNDER VIRGINIA LAW

In order to maintain a retired officer identification card with an endorsement to carry a concealed firearm, a retired deputy shall (Va. Code § 18.2-308.016):

(a) Qualify annually with the authorized firearm at a course approved by this department at the retired deputy's expense.

(b) Remain subject to all applicable department policies and federal, state and local laws.

(c) Not engage in conduct that compromises public safety.

207.6 DENIAL, SUSPENSION OR REVOCATION

A LEOSA identification card may be denied or revoked upon a showing of good cause as determined by the Department. In the event that an identification card is denied, suspended or revoked, the former deputy may request a review by the Sheriff. The decision of the Sheriff is final.

207.7 FIREARM QUALIFICATIONS

The Rangemaster will provide former deputies from this department an opportunity to qualify. Written evidence of the qualification and the weapons used will be provided and will contain the date of the qualification. The Rangemaster will maintain a record of the qualifications and weapons used (Va. Code § 18.2-308.016).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Chapter 3 - General Operations

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Use of Force

300.1 PURPOSE AND SCOPE

This policy provides guidelines on the reasonable use of force. While there is no way to specify the exact amount or type of reasonable force to be applied in any situation, every member of this department is expected to use these guidelines to make such decisions in a professional, impartial, and reasonable manner.

In addition to those methods, techniques, and tools set forth below, the guidelines for the reasonable application of force contained in this policy shall apply to all policies addressing the potential use of force, including but not limited to the Control Devices and Conducted Energy Device policies.

300.1.1 DEFINITIONS

Definitions related to this policy include:

Deadly force - Any force that is likely or intended to cause serious bodily injury or death (Va. Code § 19.2-83.3).

Feasible - Reasonably capable of being done or carried out under the circumstances to successfully achieve the arrest or lawful objective without increasing risk to the deputy or another person.

Force - The application of physical techniques or tactics, chemical agents, or weapons to another person. It is not a use of force when a person allows him/herself to be searched, escorted, handcuffed, or restrained.

Imminent - Ready to take place; impending. Note that imminent does not mean immediate or instantaneous.

Totality of the circumstances - All facts and circumstances known to the deputy at the time, taken as a whole, including the conduct of the deputy and the subject leading up to the use of force.

300.2 POLICY

The use of force by law enforcement personnel is a matter of critical concern, both to the public and to the law enforcement community. Deputies are involved on a daily basis in numerous and varied interactions and, when warranted, may use reasonable force in carrying out their duties.

Deputies must have an understanding of, and true appreciation for, their authority and limitations. This is especially true with respect to overcoming resistance while engaged in the performance of law enforcement duties.

The Madison County Sheriff's Office recognizes and respects the value of all human life and dignity without prejudice to anyone. Vesting deputies with the authority to use reasonable force and to protect the public welfare requires monitoring, evaluation, and a careful balancing of all interests.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

300.2.1 DUTY TO INTERVENE AND REPORT
Any deputy present and observing another law enforcement officer or a member using or attempting to use force that is clearly beyond that which is objectively reasonable under the circumstances shall, when in a position to do so, intervene to prevent the use of unreasonable force (Va. Code § 19.2-83.6).

Any deputy who intervenes or observes another law enforcement officer or a member use or attempt to use force that is potentially beyond that which is objectively reasonable under the circumstances shall report these observations to a supervisor as soon as feasible (Va. Code § 19.2-83.6).

300.2.2 PERSPECTIVE
When observing or reporting force used by a law enforcement officer, each deputy should take into account the totality of the circumstances and the possibility that other law enforcement officers may have additional information regarding the threat posed by the subject.

300.2.3 WRITTEN STATEMENT REGARDING INTERVENTION
Any deputy who observes another deputy use or attempt to use force that is clearly beyond that which is objectively reasonable under the circumstances shall prepare a detailed written statement consistent with the department's procedures, and the supervisor should include that statement in the supervisor's report.

300.2.4 ADMINISTRATIVE REVIEW OF INTERVENTION
An administrative review of the intervention shall be conducted by a supervisor not directly involved in the incident and reviewed by the Sheriff or the authorized designee to determine compliance with established policy.

300.3 USE OF FORCE
Deputies shall use only that amount of force that reasonably appears necessary given the facts and circumstances perceived by the deputy at the time of the event to accomplish a legitimate law enforcement purpose.

The reasonableness of force will be judged from the perspective of a reasonable deputy on the scene at the time of the incident. Any evaluation of reasonableness must allow for the fact that deputies are often forced to make split-second decisions about the amount of force that reasonably appears necessary in a particular situation, with limited information and in circumstances that are tense, uncertain and rapidly evolving.

Given that no policy can realistically predict every possible situation a deputy might encounter, deputies are entrusted to use well-reasoned discretion in determining the appropriate use of force in each incident.

It is also recognized that circumstances may arise in which deputies reasonably believe that it would be impractical or ineffective to use any of the tools, weapons or methods provided by this department. Deputies may find it more effective or reasonable to improvise their response

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

to rapidly unfolding conditions that they are confronting. In such circumstances, the use of any improvised device or method must nonetheless be reasonable and utilized only to the degree that reasonably appears necessary to accomplish a legitimate law enforcement purpose.

While the ultimate objective of every law enforcement encounter is to avoid or minimize injury, nothing in this policy requires a deputy to retreat or be exposed to possible physical injury before applying reasonable force.

300.3.1 ALTERNATIVE TACTICS - DE-ESCALATION

When circumstances reasonably permit, deputies should use non-violent strategies and techniques to decrease the intensity of a situation, improve decision-making, improve communication, reduce the need for force, and increase voluntary compliance (e.g., summoning additional resources, formulating a plan, attempting verbal persuasion).

300.3.2 FACTORS USED TO DETERMINE THE REASONABLENESS OF FORCE

When determining whether to apply force and evaluating whether a deputy has used reasonable force, a number of factors should be taken into consideration, as time and circumstances permit. These factors include but are not limited to:

(a) Immediacy and severity of the threat to deputies or others.

(b) The conduct of the individual being confronted, as reasonably perceived by the deputy at the time.

(c) Deputy/subject factors (e.g., age, size, relative strength, skill level, injuries sustained, level of exhaustion or fatigue, the number of deputies available vs. subjects).

(d) The effects of suspected drug or alcohol use.

(e) The individual’s mental state or capacity.

(f) The individual’s ability to understand and comply with deputy commands.

(g) Proximity of weapons or dangerous improvised devices.

(h) The degree to which the individual has been effectively restrained and his/her ability to resist despite being restrained.

(i) The availability of other reasonable and feasible options and their possible effectiveness.

(j) Seriousness of the suspected offense or reason for contact with the individual.

(k) Training and experience of the deputy.

(l) Potential for injury to deputies, suspects, and others.

(m) Whether the individual appears to be resisting, attempting to evade arrest by flight, or is attacking the deputy.

(n) The risk and reasonably foreseeable consequences of escape.

(o) The apparent need for immediate control of the individual or a prompt resolution of the situation.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(p) Whether the conduct of the individual being confronted no longer reasonably appears to pose an imminent threat to the deputy or others.

(q) Prior contacts with the individual or awareness of any propensity for violence.

(r) Any other exigent circumstances.

300.3.3 PAIN COMPLIANCE TECHNIQUES

Pain compliance techniques may be effective in controlling a physically or actively resisting individual. Deputies may only apply those pain compliance techniques for which they have successfully completed department-approved training. Deputies utilizing any pain compliance technique should consider:

(a) The degree to which the application of the technique may be controlled given the level of resistance.

(b) Whether the individual can comply with the direction or orders of the deputy.

(c) Whether the individual has been given sufficient opportunity to comply.

The application of any pain compliance technique shall be discontinued once the deputy determines that compliance has been achieved.

300.3.4 CAROTID CONTROL HOLD

A carotid control hold is a technique (including but not limited to a lateral vascular neck restraint) designed to control or disable an individual by temporarily restricting blood flow through the application of pressure to the neck, including the carotid artery, and, unlike a chokehold, does not restrict the airway (Va. Code § 19.2-83.4). The proper application of the carotid control hold may be effective in restraining a violent or combative individual. However, due to the potential for injury, the use of the carotid control hold is limited to those circumstances where deadly force is authorized and is subject to the following:

(a) At all times during the application of the carotid control hold, the response of the individual should be monitored. The carotid control hold should be discontinued when circumstances indicate that the application no longer reasonably appears necessary.

(b) Any individual who has had the carotid control hold applied, regardless of whether he/she was rendered unconscious, shall be promptly examined by paramedics or other qualified medical personnel and should be monitored until such examination occurs.

(c) The deputy shall inform any person receiving custody, or any person placed in a position of providing care, that the individual has been subjected to the carotid control hold and whether the individual lost consciousness as a result.

(d) Any deputy attempting or applying the carotid control hold shall promptly notify a supervisor of the use or attempted use of such hold.

(e) The use or attempted use of the carotid control hold shall be thoroughly documented by the deputy in any related reports.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

300.3.5 RESPIRATORY RESTRAINTS

A respiratory restraint, also known as a chokehold, includes the use of any body part or object to attempt to control or disable a person by applying pressure against the neck, including the trachea, with the purpose, intent, or effect of controlling or restricting the person’s movement or breathing (Va. Code § 19.2-83.4). The use of a respiratory restraint is limited to circumstances where deadly force is authorized and if applied, is subject to the same guidelines and requirements as a carotid control hold (Va. Code § 19.2-83.4).

300.3.6 USE OF FORCE TO SEIZE EVIDENCE

In general, deputies may use reasonable force to lawfully seize evidence and to prevent the destruction of evidence. However, deputies are discouraged from using force solely to prevent a person from swallowing evidence or contraband. In the instance when force is used, deputies should not intentionally use any technique that restricts blood flow to the head, restricts respiration or which creates a reasonable likelihood that blood flow to the head or respiration would be restricted. Deputies are encouraged to use techniques and methods taught by the Madison County Sheriff's Office for this specific purpose.

300.4 DEADLY FORCE APPLICATIONS

When reasonable, the deputy shall, prior to the use of deadly force, make efforts to identify him/herself as a peace officer and to warn that deadly force may be used, unless the deputy has objectively reasonable grounds to believe the person is aware of those facts.

Use of deadly force is justified in the following circumstances involving imminent threat or imminent risk:

(a) A deputy may use deadly force to protect him/herself or others from what he/she reasonably believes is an imminent threat of death or serious bodily injury.

(b) A deputy may use deadly force to stop a fleeing subject when the deputy has probable cause to believe that the individual has committed, or intends to commit, a felony involving the infliction or threatened infliction of serious bodily injury or death, and the deputy reasonably believes that there is an imminent risk of serious bodily injury or death to any other person if the individual is not immediately apprehended. Under such circumstances, a verbal warning should precede the use of deadly force, where feasible.

Imminent does not mean immediate or instantaneous. An imminent danger may exist even if the suspect is not at that very moment pointing a weapon at someone. For example, an imminent danger may exist if a deputy reasonably believes that the individual has a weapon or is attempting to access one and intends to use it against the deputy or another person. An imminent danger may also exist if the individual is capable of causing serious bodily injury or death without a weapon, and the deputy believes the individual intends to do so.

A deputy may use deadly force to stop a fleeing subject when the deputy has probable cause to believe that the individual has committed, or intends to commit, a felony involving the infliction or threatened infliction of serious bodily injury or death, and the deputy reasonably believes that there is an imminent risk of serious bodily injury or death to any

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

other person if the individual is not immediately apprehended. Under such circumstances, a verbal warning should precede the use of deadly force, where feasible.

300.4.1 STATE LIMITATIONS TO DEADLY FORCE APPLICATIONS

Prior to using deadly force, the deputy should exhaust all other reasonable options under the circumstances and, if feasible, provide a warning that deadly force may be used (Va. Code § 19.2-83.5).

In circumstances where deadly force is authorized, the necessity to protect others does not extend to the subject of the use of deadly force (Va. Code § 19.2-83.5).

300.4.2 MOVING VEHICLES

Shots fired at or from a moving vehicle involve additional considerations and risks, and are rarely effective.

When feasible, deputies should take reasonable steps to move out of the path of an approaching vehicle instead of discharging their firearm at the vehicle or any of its occupants.

A deputy should only discharge a firearm at a moving vehicle or its occupants in circumstances where deadly force is authorized (Va. Code § 19.2-83.4).

Deputies should not shoot at any part of a vehicle in an attempt to disable the vehicle.

300.5 REPORTING THE USE OF FORCE

Any use of force by a member of this department shall be documented promptly, completely, and accurately in an appropriate report, depending on the nature of the incident. The deputy should articulate the factors perceived and why he/she believed the use of force was reasonable under the circumstances.

To collect data for purposes of training, resource allocation, analysis, and related purposes, the Department may require the completion of additional report forms, as specified in department policy, procedure, or law. See the Report Preparation Policy for additional circumstances that may require documentation.

See attachment: Use of Force Report.pdf

300.5.1 NOTIFICATIONS TO SUPERVISORS

Supervisory notification shall be made as soon as practicable following the application of force in any of the following circumstances:

(a) The application caused a visible injury.

(b) The application would lead a reasonable deputy to conclude that the individual may have experienced more than momentary discomfort.

(c) The individual subjected to the force complained of injury or continuing pain.

(d) The individual indicates intent to pursue litigation.

(e) Any application of the conducted energy device or control device.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(f) Any application of a restraint device other than handcuffs, shackles, or belly chains.

(g) The individual subjected to the force was rendered unconscious.

(h) An individual was struck or kicked.

(i) An individual alleges unreasonable force was used or that any of the above has occurred.

300.6 MEDICAL CONSIDERATIONS

Once it is reasonably safe to do so, medical assistance shall be obtained for any person who exhibits signs of physical distress, has sustained visible injury, expresses a complaint of injury or continuing pain, or was rendered unconscious. Any individual exhibiting signs of physical distress after an encounter should be continuously monitored until the individual can be medically assessed. Individuals should not be placed on their stomachs for an extended period, as this could impair their ability to breathe.

Based upon the deputy's initial assessment of the nature and extent of the individual's injuries, medical assistance may consist of examination by an emergency medical services provider or medical personnel at a hospital or jail. If any such individual refuses medical attention, such a refusal shall be fully documented in related reports and, whenever practicable, should be witnessed by another deputy and/or medical personnel. If a recording is made of the contact or an interview with the individual, any refusal should be included in the recording, if possible.

The on-scene supervisor or, if the on-scene supervisor is not available, the primary handling deputy shall ensure that any person providing medical care or receiving custody of a person following any use of force is informed that the person was subjected to force. This notification shall include a description of the force used and any other circumstances the deputy reasonably believes would be potential safety or medical risks to the subject (e.g., prolonged struggle, extreme agitation, impaired respiration).

Individuals who exhibit extreme agitation, violent irrational behavior accompanied by profuse sweating, extraordinary strength beyond their physical characteristics, and imperviousness to pain, or who require a protracted physical encounter with multiple deputies to be brought under control, may be at an increased risk of sudden death. Calls involving these persons should be considered medical emergencies. Deputies who reasonably suspect a medical emergency should request medical assistance as soon as practicable and have medical personnel stage away.

See the Medical Aid and Response Policy for additional guidelines.

300.7 SUPERVISOR RESPONSIBILITIES

A supervisor should respond to a reported application of force resulting in visible injury, if reasonably available. When a supervisor is able to respond to an incident in which there has been a reported application of force, the supervisor is expected to:

(a) Obtain the basic facts from the involved deputies. Absent an allegation of misconduct or excessive force, this will be considered a routine contact in the normal course of duties.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Ensure that any injured parties are examined and treated.

(c) When possible, separately obtain a recorded interview with the individual upon whom force was applied. If this interview is conducted without the individual having voluntarily waived his/her *Miranda* rights, the following shall apply:

1. The content of the interview should not be summarized or included in any related criminal charges.
2. The fact that a recorded interview was conducted should be documented in a property or other report.
3. The recording of the interview should be distinctly marked for retention until all potential for civil litigation has expired.

(d) Once any initial medical assessment has been completed or first aid has been rendered, ensure that photographs have been taken of any areas involving visible injury or complaint of pain, as well as overall photographs of uninjured areas.

1. These photographs should be retained until all potential for civil litigation has expired.

(e) Identify any witnesses not already included in related reports.

(f) Review and approve all related reports.

(g) Determine if there is any indication that the individual may pursue civil litigation.

1. If there is an indication of potential civil litigation, the supervisor should complete and route a notification of a potential claim through the appropriate channels.

(h) Evaluate the circumstances surrounding the incident and initiate an administrative investigation if there is a question of policy noncompliance or if for any reason further investigation may be appropriate.

In the event that a supervisor is unable to respond to the scene of an incident involving the reported application of force, the supervisor is still expected to complete as many of the above items as circumstances permit.

300.7.1 SHIFT SUPERVISOR RESPONSIBILITY

The Shift Supervisor shall review each use of force by any personnel within his/her command to ensure compliance with this policy and to address any training issues.

300.8 TRAINING

Deputies will receive documented annual training on this policy and demonstrate their knowledge and understanding.

Subject to available resources, deputies should receive periodic training on:

(a) Guidelines regarding vulnerable populations, including but not limited to children, elderly, pregnant persons, and individuals with physical, mental, or intellectual disabilities.

(b) De-escalation tactics, including alternatives to force.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

300.8.1 TRAINING ON DUTY TO INTERVENE
Deputies will receive documented initial training and annual refresher training on duty to intervene.

300.9 USE OF FORCE ANALYSIS

At least annually, the Patrol Division Supervisor should prepare an analysis report on use of force incidents. The report should be submitted to the Sheriff. The report should not contain the names of deputies, suspects, or case numbers, and should include:

(a) The identification of any trends in the use of force by members.

(b) Training needs recommendations.

(c) Equipment needs recommendations.

(d) Policy revision recommendations.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Use of Force Review Boards

301.1 PURPOSE AND SCOPE

This policy establishes a process for the Madison County Sheriff's Office to review the use of force by its members.

This review process shall be in addition to any other review or investigation that may be conducted by any outside or multi-agency entity having jurisdiction over the investigation or the evaluation of the use of force.

301.2 POLICY

The Madison County Sheriff's Office will objectively evaluate the use of force by its members to ensure that their authority is used appropriately and consistent with training and policy.

301.3 REMOVAL FROM LINE DUTY ASSIGNMENT

Generally, whenever a member’s actions or use of force in an official capacity, or while using department equipment, results in death or very serious injury to another, that member will be placed in a temporary administrative assignment pending an administrative review. The Sheriff may exercise discretion and choose not to place a member in an administrative assignment.

301.4 REVIEW BOARD

The Use of Force Review Board will be convened when the use of force by a member results in very serious injury or death to another person.

The Use of Force Review Board will also investigate and review the circumstances surrounding every discharge of a firearm, whether the member was on- or off-duty, excluding training or recreational use.

The Sheriff may request the Use of Force Review Board to investigate the circumstances surrounding any use of force incident.

The Sheriff will convene the Use of Force Review Board as necessary. It will be the responsibility of the Division Supervisor to notify the Sheriff of any incidents requiring board review. The involved member's Division Supervisor will also ensure that all relevant reports, documents and materials are available for consideration and review by the board.

301.4.1 COMPOSITION OF THE BOARD

The Sheriff should staff the Use of Force Review Board with not less than three individuals from the following, as appropriate:

- Command staff representative from the involved member's chain of command
- Training Supervisor
- Department instructor for the type of weapon, device or technique used

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

The senior ranking command staff representative who is not in the same division as the involved member will serve as chairperson.

301.4.2 RESPONSIBILITIES OF THE BOARD

The Use of Force Review Board is empowered to conduct an administrative review and inquiry into the circumstances of an incident.

The board members may request further investigation, request reports be submitted for the board's review, call persons to present information and request the involved member to appear. The involved member will be notified of the meeting of the board and may choose to have a representative through all phases of the review process.

The board does not have the authority to recommend discipline.

The Sheriff will determine whether the board should delay its review until after completion of any criminal investigation, review by any prosecutorial body, filing of criminal charges, the decision not to file criminal charges or any other action. The board should be provided all relevant available material from these proceedings for its consideration.

Absent an express waiver from the involved member, no more than two designated board members may ask questions of the involved member. Other board members may provide questions to the designated board members.

The review shall be based upon those facts which were reasonably believed or known by the deputy at the time of the incident, applying any legal requirements, department policies, procedures and approved training to those facts. Facts later discovered but unknown to the involved member at the time shall neither justify nor call into question a member's decision regarding the use of force.

Any questioning of the involved member conducted by the board will be in accordance with Madison County Sheriff's Office disciplinary procedures, the Personnel Complaints Policy and any applicable state or federal law.

The board shall make one of the following recommended findings:

(a) The member's actions were within department policy and procedure.

(b) The member's actions were in violation of department policy and procedure.

A recommended finding requires a majority vote of the board. The board may also recommend additional investigations or reviews, such as disciplinary investigations, training reviews to consider whether training should be developed or revised, and policy reviews, as may be appropriate. The board chairperson will submit the written recommendation to the Sheriff.

The Sheriff shall review the recommendation, make a final determination as to whether the member's actions were within policy and procedure, and determine whether any additional actions, investigations or reviews are appropriate. If the Sheriff concludes that discipline should be considered, a disciplinary process will be initiated.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Use of Force Review Boards

At the conclusion of any additional reviews, copies of all relevant reports and information will be filed with the Sheriff.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Handcuffing and Restraints

302.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of handcuffs and other restraints during detentions and arrests.

302.2 POLICY

The Madison County Sheriff's Office authorizes the use of restraint devices in accordance with this policy, the Use of Force Policy and department training. Restraint devices shall not be used to punish, to display authority or as a show of force.

302.3 USE OF RESTRAINTS

Only members who have successfully completed Madison County Sheriff's Office-approved training on the use of restraint devices described in this policy are authorized to use these devices.

When deciding whether to use any restraint, deputies should carefully balance officer safety concerns with factors that include but are not limited to:

- The circumstances or crime leading to the arrest.
- The demeanor and behavior of the arrested person.
- The age and health of the person.
- Whether the person is known to be pregnant.
- Whether the person has a hearing or speaking disability. In such cases, consideration should be given, safety permitting, to handcuffing to the front in order to allow the person to sign or write notes.
- Whether the person has any other apparent disability.

302.3.1 RESTRAINT OF DETAINEES

Situations may arise where it may be reasonable to restrain a person who may, after brief investigation, be released without arrest. Unless arrested, the use of restraints on a person should continue only for as long as is reasonably necessary to ensure the safety of deputies and others. When deciding whether to remove restraints from a person, deputies should continuously weigh the safety interests at hand against the continuing intrusion upon the person.

Deputies shall transport persons in department vehicles with a safety barrier (unless there are provisions to transport in unmarked vehicles). The person will be secured with a safety belt in the rear seat opposite the driver, unless there are reasonable exceptions for auxiliary restraints or medical necessity.

302.3.2 RESTRAINT OF PREGNANT PERSONS

Persons who are known to be pregnant should be restrained in the least restrictive manner that is effective for officer safety. Leg irons, waist chains, or handcuffs behind the body should not be

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

used unless the deputy has a reasonable suspicion that the person may resist, attempt escape, injure self or others, or damage property.

No person who is in labor, delivery, or recovery after delivery shall be handcuffed or restrained except in extraordinary circumstances and only when a supervisor makes an individualized determination that such restraints are necessary for the safety of the arrestee, deputies, or others.

302.3.3 RESTRAINT OF JUVENILES

A juvenile under 14 years of age should not be restrained unless he/she is suspected of a dangerous felony or when the deputy has a reasonable suspicion that the juvenile may resist, attempt escape, injure him/herself, injure the deputy or damage property.

302.3.4 NOTIFICATIONS

Whenever a deputy transports a person with the use of restraints other than handcuffs, the deputy shall inform the jail staff upon arrival at the jail that restraints were used. This notification should include information regarding any other circumstances the deputy reasonably believes would be potential safety concerns or medical risks to the person (e.g., prolonged struggle, extreme agitation, impaired respiration) that may have occurred prior to, or during, transportation to the jail.

302.3.5 LONG DISTANCE TRANSPORTS

When an deputy is assigned to make a long-range transportation of a person, (e.g. an extradition), the deputy shall whenever possible utilize leg restraints and waist chains or a transport belt. Only one of the person's hands will be released during rest stops and meal breaks. The deputy should block any potential escape route while the person has a released hand.

302.4 APPLICATION OF HANDCUFFS OR PLASTIC CUFFS

Handcuffs, including temporary nylon or plastic cuffs, may be used only to restrain a person's hands to ensure officer safety.

Although recommended for most arrest and transport situations, handcuffing is discretionary and not an absolute requirement of the Department. Deputies should consider handcuffing any person they reasonably believe warrants that degree of restraint. However, deputies should not conclude that in order to avoid risk every person should be handcuffed regardless of the circumstances.

In most situations, handcuffs should be applied with the hands behind the person's back. When feasible, handcuffs should be double-locked to prevent tightening, which may cause undue discomfort or injury to the hands or wrists. Persons may be handcuffed in front when, in the judgment of the deputy, circumstances dictate that the person cannot not be reasonably handcuffed in the rear.

In situations where one pair of handcuffs does not appear sufficient to restrain the person or may cause unreasonable discomfort due to the person's size, deputies should consider alternatives, such as using an additional set of handcuffs or multiple plastic cuffs.

Handcuffs should be removed as soon as it is reasonable or after the person has been searched and is safely confined within a detention facility.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

302.5 APPLICATION OF SPIT HOODS

Spit hoods are temporary protective devices designed to prevent the wearer from biting and/or transferring or transmitting fluids (saliva and mucous) to others.

Spit hoods may be placed upon persons in custody when the deputy reasonably believes the person will bite or spit, either on a person or in an inappropriate place. They are generally used during application of a physical restraint, while the person is restrained, or during or after transport.

Deputies utilizing spit hoods should ensure that the spit hood is fastened properly to allow for adequate ventilation and that the restrained person can breathe normally. Deputies should provide assistance during the movement of a restrained person due to the potential for impairing or distorting that person's vision. Deputies should avoid comingling those wearing spit hoods with other detainees.

Spit hoods should not be used in situations where the restrained person is bleeding profusely from the area around the mouth or nose, or if there are indications that the person has a medical condition, such as difficulty breathing or vomiting. In such cases, prompt medical care should be obtained. If the person vomits while wearing a spit hood, the spit hood should be promptly removed and discarded. Persons who have been sprayed with oleoresin capsicum (OC) spray should be thoroughly decontaminated, including hair, head and clothing, prior to application of a spit hood.

Those who have been placed in a spit hood should be continually monitored and shall not be left unattended until the spit hood is removed. Spit hoods shall be discarded after each use.

302.6 APPLICATION OF AUXILIARY RESTRAINT DEVICES

Auxiliary restraint devices include transport belts, waist or belly chains, transportation chains, leg irons and other similar devices. Auxiliary restraint devices are intended for use during long-term restraint or transportation. They provide additional security and safety without impeding breathing, while permitting adequate movement, comfort and mobility.

Only department-authorized devices may be used. Any person in auxiliary restraints should be monitored as reasonably appears necessary.

302.7 APPLICATION OF LEG RESTRAINT DEVICES

Leg restraints may be used to restrain the legs of a violent or potentially violent person when it is reasonable to do so during the course of detention, arrest or transportation. Only restraint devices approved by the Department shall be used.

In determining whether to use the leg restraint, deputies should consider:

(a) Whether the deputy or others could be exposed to injury due to the assaultive or resistant behavior of a person.

(b) Whether it is reasonably necessary to protect the person from his/her own actions (e.g., hitting his/her head against the interior of the patrol vehicle, running away from the arresting deputy while handcuffed, kicking at objects or deputies).

(c) Whether it is reasonably necessary to avoid damage to property (e.g., kicking at windows of the patrol vehicle).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

302.7.1 GUIDELINES FOR USE OF LEG RESTRAINTS

When applying leg restraints, the following guidelines should be followed:

(a) If practicable, deputies should notify a supervisor of the intent to apply the leg restraint device. In all cases, a supervisor shall be notified as soon as practicable after the application of the leg restraint device.

(b) Once applied, absent a medical or other emergency, restraints should remain in place until the deputy arrives at the jail or other facility or the person no longer reasonably appears to pose a threat.

(c) Once secured, the person should be placed in a seated or upright position, secured with a safety belt, and shall not be placed on his/her stomach for an extended period, as this could reduce the person's ability to breathe.

(d) The restrained person should be continually monitored by a deputy while in the leg restraint. The deputy should ensure that the person does not roll onto and remain on his/her stomach.

(e) The deputy should look for signs of labored breathing and take appropriate steps to relieve and minimize any obvious factors contributing to this condition.

(f) When transported by emergency medical services, the restrained person should be accompanied by a deputy when requested by medical personnel. The transporting deputy should describe to medical personnel any unusual behaviors or other circumstances the deputy reasonably believes would be potential safety or medical risks to the person (e.g., prolonged struggle, extreme agitation, impaired respiration).

302.8 REQUIRED DOCUMENTATION

If a person is restrained and released without an arrest, the deputy shall document the details of the detention and the need for handcuffs or other restraints.

If a person is arrested, the use of handcuffs or other restraints shall be documented in the related report.

Deputies should document the following information in reports, as appropriate, when restraints other than handcuffs are used on a person:

(a) The factors that led to the decision to use restraints.

(b) Supervisor notification and approval of restraint use.

(c) The types of restraint used.

(d) The amount of time the person was restrained.

(e) How the person was transported and the position of the person during transport.

(f) Observations of the person's behavior and any signs of physiological problems.

(g) Any known or suspected drug use or other medical problems.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

302.9 TRAINING

Subject to available resources, the Training Supervisor should ensure that deputies receive periodic training on the proper use of handcuffs and other restraints, including:

(a) Proper placement and fit of handcuffs and other restraint devices approved for use by the Department.

(b) Response to complaints of pain by restrained persons.

(c) Options for restraining those who may be pregnant without the use of leg irons, waist chains, or handcuffs behind the body.

(d) Options for restraining amputees or those with medical conditions or other physical conditions that may be aggravated by being restrained.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Control Devices

303.1 PURPOSE AND SCOPE

This policy provides guidelines for the use and maintenance of control devices that are described in this policy.

303.2 POLICY

In order to control individuals who are violent or who demonstrate the intent to be violent, the Madison County Sheriff's Office authorizes deputies to use control devices in accordance with the guidelines in this policy and the Use of Force Policy. The Sheriff may also authorize other positions or individual department members to use specific control devices.

303.3 ISSUING, CARRYING, AND USING CONTROL DEVICES

Control devices described in this policy may be carried and used by members of this department only if the device has been issued by the Department or approved by the Sheriff or the authorized designee.

Only those members who have successfully completed department-approved training and have demonstrated proficiency in the use of any control device are authorized to carry and use the device.

Control devices may be used when a decision has been made to control, restrain, or arrest a person who is violent or who demonstrates the intent to be violent and the use of the device appears reasonable under the circumstances. When reasonable, a verbal warning and opportunity to comply should precede the use of these devices.

303.4 RESPONSIBILITIES

303.4.1 SHIFT SUPERVISOR RESPONSIBILITIES

The Shift Supervisor may authorize the use of a control device by selected department members who may not currently be issued or carrying the control device or those in specialized assignments who have successfully completed the required training.

303.4.2 RANGEMASTER RESPONSIBILITIES

The Rangemaster shall control the inventory and issuance of all control devices and shall ensure that all damaged, inoperative, outdated or expended control devices or munitions are properly disposed of, repaired or replaced.

Every control device will be periodically inspected by the Rangemaster or the designated instructor for a particular control device. The inspection shall be documented.

303.4.3 USER RESPONSIBILITIES

All normal maintenance, charging or cleaning shall remain the responsibility of personnel using the various devices.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Any damaged, inoperative, outdated or expended control devices or munitions, along with documentation explaining the cause of the damage, shall be returned to the Rangemaster for disposition. Documentation shall also be forwarded through the chain of command, when appropriate, explaining the cause of damage.

303.5 BATON GUIDELINES

The need to immediately control a suspect must be weighed against the risk of causing serious injury. The head, neck, throat, spine, heart, kidneys and groin should not be intentionally targeted except when the deputy reasonably believes the suspect poses an imminent threat of serious bodily injury or death to him/herself or others.

When carrying a baton, uniformed personnel shall carry the baton in its authorized holder on the equipment belt. Plainclothes and non-field personnel may carry the baton as authorized and in accordance with the needs of their assignments or at the direction of their supervisors.

303.6 TEAR GAS GUIDELINES

Tear gas may be used for crowd control, crowd dispersal or against barricaded suspects, based on the circumstances. Only the Sheriff or Crisis Response Unit Commander may authorize the delivery and use of tear gas, and only after evaluating all conditions known at the time and determining that such force reasonably appears justified and necessary.

When practicable, fire and emergency medical services personnel should be alerted or summoned to the scene prior to the deployment of tear gas to control any fires and to assist in providing medical aid or gas evacuation, if needed.

303.7 OLEORESIN CAPSICUM (OC) GUIDELINES

As with other control devices, OC spray and pepper projectiles may be considered for use to bring under control an individual or group of individuals who are engaging in, or are about to engage in, violent behavior. Pepper projectiles and OC spray should not, however, be used against individuals or groups who merely fail to disperse or do not reasonably appear to present a risk to the safety of department members or the public.

303.7.1 OC SPRAY

Uniformed members carrying OC spray shall carry the device in its holster on the equipment belt. Plainclothes and non-field members may carry OC spray as authorized, in accordance with the needs of their assignments or at the direction of their supervisors.

303.7.2 PEPPER PROJECTILE SYSTEMS

Pepper projectiles are plastic spheres that are filled with a derivative of OC powder. Because the compressed gas launcher delivers the projectiles with enough force to burst the projectiles on impact and release the OC powder, the potential exists for the projectiles to inflict injury if they strike the head, neck, spine or groin. Therefore, personnel using a pepper projectile system should not intentionally target those areas, except when the deputy reasonably believes the suspect poses an imminent threat of serious bodily injury or death to the deputy or others.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Deputies encountering a situation that warrants the use of a pepper projectile system shall notify a supervisor as soon as practicable. A supervisor shall respond to all pepper projectile system incidents where an individual has been hit or exposed to the chemical agent. The supervisor shall ensure that all notifications and reports are completed as required by the Use of Force Policy.

Each deployment of a pepper projectile system shall be documented. This includes situations where the launcher was directed toward an individual, whether or not the launcher was used. Unintentional discharges shall be promptly reported to a supervisor and documented on the appropriate report form. Only non-incident use of a pepper projectile system, such as training or a product demonstration, is exempt from the reporting requirement.

303.7.3 TREATMENT FOR OC EXPOSURE

Persons who have been sprayed with or otherwise affected by the use of OC should be promptly provided with clean water to cleanse the affected areas. Those who complain of further severe effects shall be examined by appropriate medical personnel.

303.8 POST-APPLICATION NOTICE

Whenever tear gas or OC has been introduced into a residence, building interior, vehicle or other enclosed area, the owners or available occupants should be provided with notice of the possible presence of residue which could result in irritation or injury if the area is not properly cleaned. Such notice should include advisement that cleanup will be at the owner’s expense. Information regarding how and when the notice was delivered and the individuals notified should be included in related reports.

303.9 KINETIC ENERGY PROJECTILE GUIDELINES

This department is committed to reducing the potential for violent confrontations. Kinetic energy projectiles, when used properly, are less likely to result in death or serious physical injury and can be used in an attempt to de-escalate a potentially deadly situation.

303.9.1 DEPLOYMENT AND USE

Only department-approved kinetic energy munitions shall be carried and deployed. Approved munitions may be used to compel an individual to cease his/her actions when such munitions present a reasonable option and provided the use complies with Virginia law (Va. Code § 19.2-83.4).

Deputies are not required or compelled to use approved munitions in lieu of other reasonable tactics if the involved deputy determines that deployment of these munitions cannot be done safely. The safety of hostages, innocent persons, and deputies takes priority over the safety of individuals engaged in criminal or suicidal behavior.

Circumstances appropriate for deployment include but are not limited to situations in which:

(a) The suspect is armed with a weapon and the tactical circumstances allow for the safe application of approved munitions.

(b) The suspect has made credible threats to harm him/herself or others.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) The suspect is engaged in riotous behavior or is throwing rocks, bottles, or other dangerous projectiles at deputies, other department members, and/or other people.

(d) There is probable cause to believe that the suspect has already committed a crime of violence and is refusing to comply with lawful orders.

303.9.2 DEPLOYMENT CONSIDERATIONS

Before discharging projectiles, the deputy should consider such factors as:

(a) Distance and angle to target.

(b) Type of munitions employed.

(c) Type and thickness of subject's clothing.

(d) The subject's proximity to others.

(e) The location of the subject.

(f) Whether the subject's actions dictate the need for an immediate response and the use of control devices appears appropriate.

A verbal warning of the intended use of the device should precede its application, unless it would otherwise endanger the safety of deputies or when it is not practicable due to the circumstances. The purpose of the warning is to give the individual a reasonable opportunity to voluntarily comply and to warn other deputies and individuals that the device is being deployed.

Deputies should keep in mind the manufacturer's recommendations and their training regarding effective distances and target areas. However, deputies are not restricted solely to use according to manufacturer recommendations. Each situation must be evaluated on the totality of circumstances at the time of deployment.

The need to immediately incapacitate the suspect must be weighed against the risk of causing serious injury or death. The head and neck should not be intentionally targeted, except when the deputy reasonably believes the suspect poses an imminent threat of serious bodily injury or death to the deputy or others.

303.9.3 SAFETY PROCEDURES

Shotguns specifically designated for use with kinetic energy projectiles will be specially marked in a manner that makes them readily identifiable as such.

Deputies will inspect shotguns and projectiles at the beginning of each shift to ensure that the shotguns are in proper working order and the projectiles are of the approved type and appear to be free from defects.

When they are not deployed, shotguns will be unloaded and properly and securely stored in sheriff's department vehicles. When deploying a kinetic energy projectile shotgun, deputies shall visually inspect the kinetic energy projectiles to ensure that conventional ammunition is not being loaded into the shotgun.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Absent compelling circumstances, deputies who must transition from conventional ammunition to kinetic energy projectiles will employ the two-person rule for loading. The two-person rule is a safety measure in which a second deputy watches the unloading and loading process to ensure that the weapon is completely emptied of conventional ammunition.

303.10 TRAINING FOR CONTROL DEVICES

The Training Supervisor shall ensure that those members who are authorized to carry a control device have been properly trained and certified to carry the specific control device and are retrained or recertified at a minimum every two years.

(a) Proficiency training shall be monitored and documented by a certified control-device weapons or tactics instructor.

(b) All training and proficiency for control devices will be documented in the member's training file.

(c) Members who fail to demonstrate proficiency with the control device or knowledge of the Use of Force Policy will be provided remedial training. If a member cannot demonstrate proficiency with a control device or knowledge of the Use of Force Policy after remedial training, the member will be restricted from carrying the control device and may be subject to discipline.

Before being authorized to carry control devices, members will be issued copies of and be instructed in applicable use of force policies, including the Control Devices Policy. Each member shall acknowledge that they have been provided access to and have had the opportunity to review and understand the applicable policies.

303.11 REPORTING USE OF CONTROL DEVICES

Any application of a control device shall be documented in the related incident report and reported pursuant to the Use of Force Policy.

See attachment: Use of Force Report.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Conducted Energy Device

304.1 PURPOSE AND SCOPE

This policy provides guidelines for the issuance and use of the conducted energy device (CED).

304.2 POLICY

The CED is used in an attempt to control a violent or potentially violent individual. The appropriate use of such a device may result in fewer serious injuries to deputies and suspects.

304.3 ISSUANCE AND CARRYING CEDS

Only members who have successfully completed department-approved training and have demonstrated proficiency may be issued and may carry the CED.

The Rangemaster should keep a log of issued CED devices and the serial numbers of cartridges/magazines issued to members.

CEDs are issued for use during a member's current assignment. Those leaving a particular assignment may be required to return the device to the department inventory.

Deputies shall only use the CED and cartridges/magazines that have been issued by the Department. Cartridges/magazines should not be used after the manufacturer's expiration date.

Uniformed deputies who have been issued the CED shall wear the device in an approved holster.

Deputies who carry the CED while in uniform shall carry it in a holster on the side opposite the duty weapon.

(a) All CEDs shall be clearly distinguishable to differentiate them from the duty weapon and any other device.

(b) For single-shot devices, whenever practicable, deputies should carry an additional cartridge on their person when carrying the CED.

(c) Deputies should not hold a firearm and the CED at the same time.

Non-uniformed deputies may secure the CED in a concealed, secure location in the driver's compartment of their vehicles.

304.3.1 USER RESPONSIBILITIES

Deputies shall be responsible for ensuring that the issued CED is properly maintained and in good working order. This includes a function test and battery life monitoring, as required by the manufacturer, and should be completed prior to the beginning of the deputy's shift.

CEDs that are damaged or inoperative, or cartridges/magazines that are expired or damaged, shall be returned to the Rangemaster for disposition. Deputies shall submit documentation stating the reason for the return and how the CED or cartridge/magazine was damaged or became inoperative, if known.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

304.4 VERBAL AND VISUAL WARNINGS

A verbal warning of the intended use of the CED should precede its application, unless it would otherwise endanger the safety of deputies or when it is not practicable due to the circumstances. The purpose of the warning is to:

(a) Provide the individual with a reasonable opportunity to voluntarily comply.

(b) Provide other deputies and individuals with a warning that the CED may be deployed.

If, after a verbal warning, an individual fails to voluntarily comply with a deputy's lawful orders and it appears both reasonable and feasible under the circumstances, the deputy may, but is not required to, activate any warning on the device, which may include display of the electrical arc, an audible warning, or the laser in a further attempt to gain compliance prior to the application of the CED. The laser should not be intentionally directed into anyone's eyes.

The fact that a verbal or other warning was given or the reasons it was not given shall be documented by the deputy deploying the CED in the related report.

304.5 USE OF THE CED

The CED has limitations and restrictions requiring consideration before its use. The CED should only be used when its operator can safely deploy the device within its operational range. Although the CED may be effective in controlling most individuals, deputies should be aware that the device may not achieve the intended results and be prepared with other options.

If sufficient personnel are available and can be safely assigned, a deputy designated as lethal cover for any deputy deploying a CED may be considered for officer safety.

304.5.1 APPLICATION OF THE CED

The CED may be used when the circumstances reasonably perceived by the deputy at the time indicate that such application reasonably appears necessary to control a person who:

(a) Is violent or is physically resisting.

(b) Has demonstrated, by words or action, an intention to be violent or to physically resist, and reasonably appears to present the potential to harm deputies, themself, or others.

Mere flight from a pursuing deputy, without additional circumstances or factors, is not good cause for the use of the CED to apprehend an individual.

The CED shall not be used to psychologically torment, to elicit statements, or to punish any individual.

304.5.2 SPECIAL DEPLOYMENT CONSIDERATIONS

The use of the CED on certain individuals should generally be avoided unless the totality of the circumstances indicates that other available options reasonably appear ineffective or would present a greater danger to the deputy, the subject, or others, and the deputy reasonably believes that the need to control the individual outweighs the potential risk of using the device. This includes:

(a) Individuals who are known to be pregnant.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Elderly individuals or obvious juveniles.

(c) Individuals with obviously low body mass.

(d) Individuals who are handcuffed or otherwise restrained.

(e) Individuals known to have been recently sprayed with a flammable chemical agent or who are otherwise known to be in close proximity to any known combustible vapor or flammable material, including alcohol-based oleoresin capsicum (OC) spray.

(f) Individuals whose position or activity is likely to result in collateral injury (e.g., falls from height, located in water, operating vehicles).

Any CED capable of being applied in the drive-stun mode (i.e., direct contact without probes as a primary form of pain compliance) should be limited to supplementing the probe-mode to complete the circuit, or as a distraction technique to gain separation between deputies and the subject, thereby giving deputies time and distance to consider other force options or actions.

304.5.3 TARGETING CONSIDERATIONS

Recognizing that the dynamics of a situation and movement of the subject may affect target placement of probes, when practicable, deputies should attempt to target the back, lower center mass, and upper legs of the subject, and avoid intentionally targeting the head, neck, area of the heart, or genitals. If circumstances result in one or more probes inadvertently striking an area outside of the preferred target zones, the individual should be closely monitored until examined by paramedics or other medical personnel.

304.5.4 MULTIPLE APPLICATIONS OF THE CED

Once a deputy has successfully deployed two probes on the subject, the deputy should continually assess the subject to determine if additional probe deployments or cycles reasonably appear necessary. Additional factors deputies may consider include but are not limited to:

(a) Whether it is reasonable to believe that the need to control the individual outweighs the potentially increased risk posed by multiple applications.

(b) Whether the probes are making proper contact.

(c) Whether the individual has the ability and has been given a reasonable opportunity to comply.

(d) Whether verbal commands or other options or tactics may be more effective.

Given that on certain devices (e.g., TASER 10™) each trigger pull deploys a single probe, the deputy must pull the trigger twice to deploy two probes to create the possibility of neuro-muscular incapacitation.

304.5.5 ACTIONS FOLLOWING DEPLOYMENTS

Deputies should take appropriate actions to control and restrain the individual as soon as reasonably practicable to minimize the need for longer or multiple exposures to the CED. As soon as practicable, deputies shall notify a supervisor any time the CED has been discharged. If needed for evidentiary purposes, the expended cartridge, along with any probes and wire, should

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

be submitted into evidence (including confetti tags, when equipped on the device). The evidence packaging should be marked "Biohazard" if the probes penetrated the subject's skin.

304.5.6 DANGEROUS ANIMALS
The CED may be deployed against an animal if the animal reasonably appears to pose an imminent threat to human safety.

304.5.7 OFF-DUTY CONSIDERATIONS
Deputies are not authorized to carry department CEDs while off-duty.

Deputies shall ensure that CEDs are secured while in their homes, vehicles, or any other area under their control, in a manner that will keep the device inaccessible to others.

304.6 DOCUMENTATION

Deputies shall document all CED discharges in the related arrest/crime reports and the CED report forms. Photographs should be taken of any obvious probe impact or drive-stun application sites and attached to the CED report form. Notification shall also be made to a supervisor in compliance with the Use of Force Policy. Unintentional discharges, pointing the device at a person, audible warning, laser activation, and arcing the device, other than for testing purposes, will also be documented on the report form. Data downloads from the CED after use on a subject should be done as soon as practicable using a department-approved process to preserve the data.

304.6.1 CED REPORT FORM
As applicable based on the device type, items that shall be included in the CED report form are:

(a) The brand, model, and serial number of the CED and any cartridge/magazine.

(b) Date, time, and location of the incident.

(c) Whether any warning, display, laser, or arc deterred a subject and gained compliance.

(d) The number of probes deployed, CED activations, the duration of each cycle, the duration between activations, and (as best as can be determined) the duration that the subject received applications.

(e) The range at which the CED was used.

(f) The type of mode used (e.g., probe deployment, drive-stun).

(g) Location of any probe impact.

(h) Location of contact in drive-stun mode.

(i) Description of where missed probes went.

(j) Whether medical care was provided to the subject.

(k) Whether the subject sustained any injuries.

(l) Whether any deputies sustained any injuries.

The Training Supervisor should periodically analyze the report forms to identify trends, including deterrence and effectiveness. The Training Supervisor should also conduct audits of CED

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

device data downloaded to an approved location and reconcile CED report forms with recorded activations. CED information and statistics, with identifying information removed, should periodically be made available to the public.

304.6.2 REPORTS

The deputy should include the following in the arrest/crime report:

(a) Identification of all personnel firing CEDs

(b) Identification of all witnesses

(c) Medical care provided to the subject

(d) Observations of the subject's physical and physiological actions

(e) Any known or suspected drug use, intoxication, or other medical problems

304.7 MEDICAL TREATMENT

Consistent with local medical personnel protocols and absent extenuating circumstances, only appropriate medical personnel or deputies trained in probe removal and handling should remove CED probes from a person's body. Used CED probes shall be treated as a sharps biohazard, similar to a used hypodermic needle, and handled appropriately. Universal precautions should be taken.

All persons who have been struck by CED probes, who have been subjected to the electric discharge of the device, or who sustained direct exposure of the laser to the eyes shall be medically assessed prior to booking. Additionally, any such individual who falls under any of the following categories should, as soon as practicable, be examined by paramedics or other qualified medical personnel:

(a) The person is suspected of being under the influence of controlled substances and/or alcohol.

(b) The person may be pregnant.

(c) The person reasonably appears to be in need of medical attention.

(d) The CED probes are lodged in a sensitive area (e.g., groin, female breast, head, face, neck).

(e) The person requests medical treatment.

Any individual exhibiting signs of distress or who is exposed to multiple or prolonged applications shall be transported to a medical facility for examination or medically evaluated prior to booking. If any individual refuses medical attention, such a refusal should be witnessed by another deputy and/or medical personnel and shall be fully documented in related reports. If an audio/video recording is made of the contact or an interview with the individual, any refusal should be included, if possible.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

The transporting deputy shall inform any person providing medical care or receiving custody that the individual has been subjected to the application of the CED (see the Medical Aid and Response Policy).

304.8 SUPERVISOR RESPONSIBILITIES

When possible, supervisors should respond to calls when they reasonably believe there is a likelihood the CED may be used. A supervisor should respond to all incidents where the CED was activated.

A supervisor should review each incident where a person has been exposed to a CED. The device's internal logs should be downloaded by a supervisor or Rangemaster and saved with the related arrest/crime report. The supervisor should arrange for photographs of probe sites to be taken and witnesses to be interviewed.

304.9 TRAINING

Personnel who are authorized to carry the CED shall be permitted to do so only after successfully completing the initial department-approved training. Any personnel who have not carried the CED as a part of their assignments for a period of six months or more shall be recertified by a qualified CED instructor prior to again carrying or using the device.

Proficiency training for personnel who have been issued CEDs should occur every year. A reassessment of a deputy's knowledge and/or practical skills may be required at any time, if deemed appropriate, by the Training Supervisor. All training and proficiency for CEDs will be documented in the deputy's training files.

Command staff, supervisors, and investigators should receive CED training as appropriate for the investigations they conduct and review.

Deputies who do not carry CEDs should receive training that is sufficient to familiarize them with the device and with working with deputies who use the device.

The Training Supervisor is responsible for ensuring that all members who carry CEDs have received initial and annual proficiency training. Periodic audits should be used for verification.

Application of CEDs during training could result in injuries and should not be mandatory for certification.

The Training Supervisor should include the following training:

(a) A review of this policy

(b) A review of the Use of Force Policy

(c) Performing weak-hand draws or cross-draws until proficient to reduce the possibility of unintentionally drawing and firing a firearm

(d) Target area considerations, to include techniques or options to reduce the unintentional application of probes to the head, neck, area of the heart, and groin

(e) Scenario-based training, including virtual reality training when available

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(f) Handcuffing a subject during the application of the CED and transitioning to other force options

(g) De-escalation techniques

(h) Restraint techniques that do not impair respiration following the application of the CED

(i) Proper use of cover and concealment during deployment of the CED for purposes of officer safety

(j) Proper tactics and techniques related to multiple applications of CEDs

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Officer-Involved Shootings and Deaths

305.1 PURPOSE AND SCOPE

The purpose of this policy is to establish policy and procedures for the investigation of an incident in which a person is injured or dies as the result of an officer-involved shooting or dies as a result of another action of a deputy.

In other incidents not covered by this policy, the Sheriff may decide that the investigation will follow the process provided in this policy.

305.2 POLICY

The policy of the Madison County Sheriff's Office is to ensure that officer-involved shootings and deaths are investigated in a thorough, fair and impartial manner.

305.3 TYPES OF INVESTIGATIONS

Officer-involved shootings and deaths involve several separate investigations. The investigations may include:

- A criminal investigation of the suspect's actions.
- A criminal investigation of the involved officer's actions.
- An administrative investigation as to policy compliance by involved deputies.
- A civil investigation to determine potential liability.

305.4 CONTROL OF INVESTIGATIONS

Investigators from surrounding agencies may be assigned to work on the criminal investigation of officer-involved shootings and deaths. This may include at least one investigator from the agency that employs the involved officer.

Jurisdiction is determined by the location of the shooting or death and the agency employing the involved officer. The following scenarios outline the jurisdictional responsibilities for investigating officer-involved shootings and deaths.

305.4.1 CRIMINAL INVESTIGATION OF SUSPECT ACTIONS

The investigation of any possible criminal conduct by the suspect is controlled by the agency in whose jurisdiction the suspect’s crime occurred. For example, the Madison County Sheriff's Office would control the investigation if the suspect’s crime occurred in Madison County, Virginia.

If multiple crimes have been committed in multiple jurisdictions, identification of the agency that will control the investigation may be reached in the same way as with any other crime. The investigation may be conducted by the agency in control of the criminal investigation of the involved officer, at the discretion of the Sheriff and with concurrence from the other agency.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

305.4.2 CRIMINAL INVESTIGATIONS OF OFFICER ACTIONS

The control of the criminal investigation into the involved deputy's conduct during the incident will be determined by the employing agency's protocol. When a deputy from this department is involved, the criminal investigation will be handled according to the Criminal Investigation section of this policy.

Requests made of this department to investigate a shooting or death involving an outside agency's officer shall be referred to the Sheriff or the authorized designee for approval.

305.4.3 ADMINISTRATIVE AND CIVIL INVESTIGATION

Regardless of where the incident occurs, the administrative and civil investigation of each involved officer is controlled by the respective employing agency.

305.5 INVESTIGATION PROCESS

The following procedures are guidelines used in the investigation of an officer-involved shooting or death.

305.5.1 UNINVOLVED DEPUTY RESPONSIBILITIES

Upon arrival at the scene of an officer-involved shooting or death, the first uninvolved MCSO deputy will be the deputy-in-charge and will assume the responsibilities of a supervisor until properly relieved. This deputy should, as appropriate:

(a) Secure the scene and identify and eliminate hazards for all those involved.

(b) Take reasonable steps to obtain emergency medical attention for injured individuals.

(c) Request additional resources from the Department or other agencies

(d) Coordinate a perimeter or pursuit of suspects.

(e) Check for injured persons and evacuate as needed.

(f) Brief the supervisor upon arrival.

305.5.2 SUPERVISOR RESPONSIBILITIES

Upon arrival at the scene, the first uninvolved MCSO supervisor should ensure completion of the duties as outlined above, plus:

(a) Attempt to obtain a brief overview of the situation from any uninvolved deputies.

1. In the event that there are no uninvolved deputies who can supply adequate overview, the supervisor should attempt to obtain a brief voluntary overview from one involved officer.

(b) If necessary, the supervisor may administratively order any MCSO deputy to immediately provide public safety information necessary to secure the scene, identify injured parties and pursue suspects.

1. Public safety information shall be limited to such things as outstanding suspect information, number and direction of any shots fired, perimeter of the incident

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

scene, identity of known or potential witnesses and any other pertinent information.

2. The initial on-scene supervisor should not attempt to order any involved officer to provide any information other than public safety information.

(c) Provide all available information to the Shift Supervisor and the Dispatch Center. If feasible, sensitive information should be communicated over secure networks.

(d) Take command of and secure the incident scene with additional MCSO members until properly relieved by another supervisor or other assigned personnel or investigator.

(e) As soon as practicable, ensure that involved officers are transported (separately, if feasible) to a suitable location for further direction.

1. Each involved MCSO deputy should be given an administrative order not to discuss the incident with other involved officers or MCSO members pending further direction from a supervisor.

2. When an involved officer's weapon is taken or left at the scene for other than officer-safety reasons (e.g., evidence), ensure that he/she is provided with a comparable replacement weapon or transported by other deputies.

305.5.3 SHIFT SUPERVISOR RESPONSIBILITIES

Upon learning of an officer-involved shooting or death, the Shift Supervisor shall be responsible for coordinating all aspects of the incident until he/she is relieved by the Sheriff or the Captain.

All outside inquiries about the incident shall be directed to the Sheriff.

305.5.4 NOTIFICATIONS

The following persons shall be notified as soon as practicable:

- Sheriff
- Captain
- Investigation Division Supervisor
- Outside agency investigators (if appropriate)
- Internal Affairs Unit supervisor
- Psychological/peer support personnel
- Chaplain
- Medical Examiner (if necessary)
- Public Information Officer

305.5.5 INVOLVED OFFICERS

The following shall be considered for the involved officer:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) Any request for legal representation will be accommodated.

1. Involved MCSO deputies shall not be permitted to meet collectively or in a group with an attorney or any representative prior to providing a formal interview or report.

2. Requests from involved non-MCSO officers should be referred to their employing agency.

(b) Discussions with licensed attorneys will be considered privileged as attorney-client communications (Va. Code § 8.01-420.7).

(c) A licensed psychotherapist shall be provided by the Department to each involved MCSO deputy. A licensed psychotherapist may also be provided to any other affected MCSO members, upon request.

1. Interviews with a licensed psychotherapist will be considered privileged (Va. Code § 8.01-399; Va. Code § 8.01-400.2).

2. An interview or session with a licensed psychotherapist may take place prior to the member providing a formal interview or report. However, the involved members shall not be permitted to consult or meet collectively or in a group with a licensed psychotherapist prior to providing a formal interview or report.

3. A separate fitness-for-duty exam may also be required (see the Fitness for Duty Policy).

(d) Communications between the involved deputy and a peer support member is addressed in the Wellness Program Policy.

Care should be taken to preserve the integrity of any physical evidence present on the involved officer's equipment or clothing, such as blood or fingerprints, until investigators or lab personnel can properly retrieve it.

Each involved MCSO deputy shall be given reasonable paid administrative leave following an officer-involved shooting or death. It shall be the responsibility of the Shift Supervisor to make schedule adjustments to accommodate such leave.

305.6 CRIMINAL INVESTIGATION

The Virginia State Police is responsible for the criminal investigation into the circumstances of any officer-involved shooting involving injury or death.

If available, investigative personnel from this department may be assigned to partner with investigators from the Virginia State Police to avoid duplicating efforts in related criminal investigations.

Once public safety issues have been addressed, criminal investigators should be given the opportunity to obtain a voluntary statement from involved officers and to complete their interviews. The following shall be considered for the involved officer:

(a) MCSO supervisors and Internal Affairs Unit personnel should not participate directly in any voluntary interview of MCSO deputies. This will not prohibit such personnel from monitoring interviews or providing the criminal investigators with topics for inquiry.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) If requested, any involved officer will be afforded the opportunity to consult individually with an attorney prior to speaking with criminal investigators. However, in order to maintain the integrity of each involved officer's statement, he/she shall not consult or meet with an attorney collectively or in groups prior to being interviewed.

(c) If any involved officer is physically, emotionally or otherwise not in a position to provide a voluntary statement when interviewed by criminal investigators, consideration should be given to allowing a reasonable period for the officer to schedule an alternate time for the interview.

(d) Any voluntary statement provided by an involved officer will be made available for inclusion in any related investigation including administrative investigations. However, no administratively coerced statement will be provided to any criminal investigators unless the officer consents.

305.6.1 REPORTS BY INVOLVED MCSO DEPUTIES

In the event that suspects remain outstanding or subject to prosecution for related offenses, this department shall retain the authority to require involved MCSO deputies to provide sufficient information for related criminal reports to facilitate the apprehension and prosecution of those individuals.

While the involved MCSO deputy may write the report, it is generally recommended that such reports be completed by assigned investigators, who should interview all involved officers as victims/witnesses. Since the purpose of these reports will be to facilitate criminal prosecution, statements of involved officers should focus on evidence to establish the elements of criminal activities by suspects. Care should be taken not to duplicate information provided by involved officers in other reports.

Nothing in this section shall be construed to deprive an involved MCSO deputy of the right to consult with legal counsel prior to completing any such criminal report.

Reports related to the prosecution of criminal suspects will be processed according to normal procedures but should also be included for reference in the investigation of the officer-involved shooting or death.

305.6.2 WITNESS IDENTIFICATION AND INTERVIEWS

Because potential witnesses to an officer-involved shooting or death may become unavailable or the integrity of their statements compromised with the passage of time, a supervisor should take reasonable steps to promptly coordinate with criminal investigators to utilize available law enforcement personnel for the following:

(a) Identification of all persons present at the scene and in the immediate area.

1. When feasible, a recorded statement should be obtained from those persons who claim not to have witnessed the incident but who were present at the time it occurred.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. Any potential witness who is unwilling or unable to remain available for a formal interview should not be detained absent reasonable suspicion to detain or probable cause to arrest. Without detaining the individual for the sole purpose of identification, attempts to identify the witness prior to his/her departure should be made whenever feasible.

(b) Witnesses who are willing to provide a formal interview should be asked to meet at a suitable location where criminal investigators may obtain a recorded statement. Such witnesses, if willing, may be transported by a member of the Department.

1. A written, verbal or recorded statement of consent should be obtained prior to transporting a witness. When the witness is a minor, consent should be obtained from the parent or guardian, if available, prior to transportation.

(c) Promptly contacting the suspect's known family and associates to obtain any available and untainted background information about the suspect's activities and state of mind prior to the incident.

305.6.3 INVESTIGATIVE PERSONNEL

Once notified of an officer-involved shooting or death, it shall be the responsibility of the designated Investigation Division supervisor to assign appropriate investigative personnel to handle the investigation of related crimes. Department investigators will be assigned to work with investigators from the the Virginia State Police and may be assigned to separately handle the investigation of any related crimes not being investigated by the Virginia State Police.

All related department reports, except administrative and/or privileged reports, will be forwarded to the designated Investigation Division supervisor for approval. Privileged reports shall be maintained exclusively by members who are authorized such access. Administrative reports will be forwarded to the appropriate Division Supervisor.

305.7 ADMINISTRATIVE INVESTIGATION

In addition to all other investigations associated with an officer-involved shooting or death, this department will conduct an internal administrative investigation of involved MCSO deputies to determine conformance with department policy. This investigation will be conducted under the supervision of the Internal Affairs Unit and will be considered a confidential deputy personnel file.

Interviews of members shall be subject to department policies and applicable laws.

(a) Any deputy involved in a shooting or death may be requested or administratively compelled to provide a blood sample for alcohol/drug screening. Absent consent from the deputy, such compelled samples and the results of any such testing shall not be disclosed to any criminal investigative agency.

(b) If any deputy has voluntarily elected to provide a statement to criminal investigators, the assigned administrative investigator should review that statement before proceeding with any further interview of that involved deputy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1. If a further interview of the deputy is deemed necessary to determine policy compliance, care should be taken to limit the inquiry to new areas with minimal, if any, duplication of questions addressed in the voluntary statement. The involved deputy shall be provided with a copy of his/her prior statement before proceeding with any subsequent interviews.

(c) In the event that an involved deputy has elected not to provide criminal investigators with a voluntary statement, the assigned administrative investigator shall conduct an administrative interview to determine all relevant information.

1. Although this interview should not be unreasonably delayed, care should be taken to ensure that the deputy's physical and psychological needs have been addressed before commencing the interview.
2. If requested, the deputy shall have the opportunity to select an uninvolved representative to be present during the interview. However, in order to maintain the integrity of each individual deputy's statement, involved deputies shall not consult or meet with a representative collectively or in groups prior to being interviewed.
3. Administrative interviews should be recorded by the investigator. The deputy may also record the interview.
4. The deputy shall be informed of the nature of the investigation. If a deputy refuses to answer questions, he/she should be given his/her *Garrity* rights and ordered to provide full and truthful answers to all questions. The deputy shall be informed that the interview will be for administrative purposes only and that the statement cannot be used criminally.
5. The Internal Affairs Unit shall compile all relevant information and reports necessary for the Department to determine compliance with applicable policies.
6. Regardless of whether the use of force is an issue in the case, the completed administrative investigation shall be submitted to the Use of Force Review Board, which will restrict its findings as to whether there was compliance with the Use of Force Policy.
7. Any other indications of potential policy violations shall be determined in accordance with standard disciplinary procedures.

305.8 CIVIL LIABILITY RESPONSE

A member of this department may be assigned to work exclusively under the direction of the legal counsel for the Department to assist in the preparation of materials deemed necessary in anticipation of potential civil litigation.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

All materials generated in this capacity shall be considered attorney work product and may not be used for any other purpose. The civil liability response is not intended to interfere with any other investigation but shall be given reasonable access to all other investigations.

305.9 AUDIO AND VIDEO RECORDINGS

Any officer involved in a shooting or death may be permitted to review available Mobile Audio/ Video (MAV), body-worn video, or other video or audio recordings prior to providing a recorded statement or completing reports.

Upon request, non-law enforcement witnesses who are able to verify their presence and their ability to contemporaneously perceive events at the scene of an incident may also be permitted to review available MAV, body-worn video, or other video or audio recordings with the approval of assigned investigators or a supervisor.

Any MAV, body-worn video, and other known video or audio recordings of an incident should not be publicly released during an ongoing investigation without consulting the Commonwealth Attorney's Office or assigned counsel, as appropriate.

305.10 DEBRIEFING

Following an officer-involved shooting or death, the Madison County Sheriff's Office should conduct both a Critical Incident Stress Debriefing and a tactical debriefing. See the Wellness Program Policy for guidance on Critical Incident Stress Debriefings.

305.10.1 TACTICAL DEBRIEFING

A tactical debriefing should take place to identify any training or areas of policy that need improvement. The Sheriff should identify the appropriate participants. This debriefing should not be conducted until all involved members have provided recorded or formal statements to the criminal and/or administrative investigators.

305.11 MEDIA RELATIONS

Any media release shall be prepared with input and concurrence from the supervisor and the department representative responsible for each phase of the investigation. Releases will be available to the Shift Supervisor, Investigation Division Supervisor and Public Information Officer in the event of inquiries from the media.

No involved MCSO deputy shall make any comment to the media unless he/she is authorized by the Sheriff or a Division Supervisor.

Department members receiving inquiries regarding officer-involved shootings or deaths occurring in other jurisdictions shall refrain from public comment and will direct those inquiries to the agency having jurisdiction and primary responsibility for the investigation.

305.12 REPORTING

If the death of an individual occurs in the Madison County Sheriff's Office jurisdiction and qualifies to be reported to the Virginia Violent Death Reporting System, the Patrol Division Supervisor

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

will ensure that the Records Manager is provided with enough information to meet the reporting requirements.

The Records Manager should also ensure that information related to any officer-involved shooting resulting in death or serious bodily injury is forwarded to the Virginia Department of State Police as soon as practicable (Va. Code § 52-28.2).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Firearms

306.1 PURPOSE AND SCOPE

This policy provides guidelines for issuing firearms, the safe and legal carrying of firearms, firearms maintenance and firearms training.

This policy does not apply to issues related to the use of a firearm that are addressed in the Use of Force or Officer-Involved Shootings and Deaths policies.

This policy only applies to those members who are authorized to carry firearms.

306.2 POLICY

The Madison County Sheriff's Office will equip its members with firearms to address the risks posed to the public and department members by violent and sometimes well-armed persons. The Department will ensure firearms are appropriate and in good working order and that relevant training is provided as resources allow.

306.3 AUTHORIZED FIREARMS, AMMUNITION, AND OTHER WEAPONS

Members shall only use firearms that are issued or approved by the Department and have been thoroughly inspected by the Rangemaster. Except in an emergency, only members receiving training and demonstrating proficiency in the use of department-authorized firearms shall be approved to carry such weapons.

All other weapons not provided by the Department, including but not limited to edged weapons, chemical or electronic weapons, impact weapons, or any weapon prohibited or restricted by law or that is not covered elsewhere by department policy, may not be carried by members in the performance of their official duties without the express written authorization of the member's Division Supervisor and demonstration of proficiency in the use of the weapon. This exclusion does not apply to the carrying of a single folding pocketknife that is not otherwise prohibited by law.

306.3.1 HANDGUNS

The authorized department-issued handgun is the Glock Model 45 9mm. The following additional handguns are approved for on-duty use:

Glock	Model 43	9 mm
Glock	Model 48	9 mm

306.3.2 SHOTGUNS

The authorized department-issued shotgun is the Remington 870P 12 Gauge. When not deployed, the shotgun shall be properly secured in a locked patrol vehicle with the magazine loaded, the action closed on an empty chamber, and the safety in the safe position.

306.3.3 PATROL RIFLES

The authorized department-issued patrol rifle is the Colt AR-15 Type .223. The following additional patrol rifles are approved for on-duty use:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Members may deploy the patrol rifle in any circumstance where the member can articulate a reasonable expectation that the rifle may be needed. Examples of some general guidelines for deploying the patrol rifle may include, but are not limited to:

(a) Situations where the member reasonably anticipates an armed encounter.

(b) When a member is faced with a situation that may require accurate and effective fire at long range.

(c) Situations where a member reasonably expects the need to meet or exceed a suspect's firepower.

(d) When a member reasonably believes that there may be a need to fire on a barricaded person or a person with a hostage.

(e) When a member reasonably believes that a suspect may be wearing body armor.

(f) When authorized or requested by a supervisor.

(g) When needed to euthanize an animal.

When not deployed, the patrol rifle shall be properly secured in a locked patrol vehicle with the chamber empty, magazine loaded and inserted into the magazine well, the bolt forward with the dust cover closed, and the selector lever in the safe position.

306.3.4 PERSONALLY OWNED DUTY FIREARMS

Members desiring to carry an authorized but personally owned duty firearm must receive written approval from the Sheriff or the authorized designee. Once approved, personally owned duty firearms are subject to the following restrictions:

(a) The firearm shall be in good working order and on the department list of approved firearms.

(b) The firearm shall be inspected by the Rangemaster prior to being carried and thereafter shall be subject to inspection whenever it is deemed necessary.

(c) Prior to carrying the firearm, members shall qualify under range supervision and thereafter shall qualify in accordance with the department's annual qualification schedule. Members must demonstrate proficiency and safe handling, and that the firearm functions properly.

(d) Members shall provide written notice of the make, model, color, serial number, and caliber of the firearm to the Rangemaster, who will maintain a list of the information.

306.3.5 AUTHORIZED SECONDARY HANDGUN

Members desiring to carry department or personally owned secondary handguns are subject to the following restrictions:

(a) The handgun shall be in good working order and on the department list of approved firearms.

(b) Only one secondary handgun may be carried at a time.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) The purchase of the handgun and ammunition shall be the responsibility of the member unless the handgun and ammunition are provided by the Department.

(d) The handgun shall be carried concealed at all times and in such a manner as to prevent unintentional cocking, discharge or loss of physical control.

(e) The handgun shall be inspected by the Rangemaster prior to being carried and thereafter shall be subject to inspection whenever it is deemed necessary.

(f) Ammunition shall be the same as department issue. If the caliber of the handgun is other than department issue, the Sheriff or the authorized designee shall approve the ammunition.

(g) Prior to carrying the secondary handgun, members shall qualify under range supervision and thereafter shall qualify in accordance with the department qualification schedule. Members must demonstrate proficiency and safe handling, and that the handgun functions properly.

(h) Members shall provide written notice of the make, model, color, serial number and caliber of a secondary handgun to the Rangemaster, who will maintain a list of the information.

306.3.6 AUTHORIZED OFF-DUTY FIREARMS

The carrying of firearms by members while off-duty is permitted by the Sheriff but may be rescinded should circumstances dictate (e.g., administrative leave). Members who choose to carry a firearm while off-duty, based on their authority as law enforcement officers, will be required to meet the following guidelines:

(a) A personally owned firearm shall be used, carried and inspected in accordance with the Personally Owned Duty Firearms requirements in this policy.

1. The purchase of the personally owned firearm and ammunition shall be the responsibility of the member.

(b) The firearm shall be carried concealed at all times and in such a manner as to prevent unintentional cocking, discharge or loss of physical control.

(c) It will be the responsibility of the member to submit the firearm to the Rangemaster for inspection prior to being personally carried. Thereafter the firearm shall be subject to periodic inspection by the Rangemaster.

(d) Prior to carrying any off-duty firearm, the member shall demonstrate to the Rangemaster that he/she is proficient in handling and firing the firearm and that it will be carried in a safe manner.

(e) The member will successfully qualify with the firearm prior to it being carried.

(f) Members shall provide written notice of the make, model, color, serial number and caliber of the firearm to the Rangemaster, who will maintain a list of the information.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(g) If a member desires to use more than one firearm while off-duty, he/she may do so, as long as all requirements set forth in this policy for each firearm are met.

(h) Members shall only carry department-authorized ammunition.

(i) When armed, deputies shall carry their badges and Madison County Sheriff's Office identification cards under circumstances requiring possession of such identification.

306.3.7 AMMUNITION

Members shall carry only department-authorized ammunition. Members shall be issued fresh duty ammunition in the specified quantity for all department-issued firearms during the member's firearms qualification. Replacements for unserviceable or depleted ammunition issued by the Department shall be dispensed by the Rangemaster when needed, in accordance with established policy.

Members carrying personally owned authorized firearms of a caliber differing from department-issued firearms shall be responsible for obtaining fresh duty ammunition in accordance with the above, at their own expense.

306.4 EQUIPMENT

Firearms carried on- or off-duty shall be maintained in a clean, serviceable condition. Maintenance and repair of authorized personally owned firearms are the responsibility of the individual member.

306.4.1 REPAIRS OR MODIFICATIONS

Each member shall be responsible for promptly reporting any damage or malfunction of an assigned firearm to a supervisor or the Rangemaster.

Firearms that are the property of the Department or personally owned firearms that are approved for department use may be repaired or modified only by a person who is department-approved and certified as an armorer or gunsmith in the repair of the specific firearm. Such modification or repair must be authorized in advance by the Rangemaster.

Any repairs or modifications to the member's personally owned firearm shall be done at his/her expense and must be approved by the Rangemaster.

306.4.2 HOLSTERS

Only department-approved holsters shall be used and worn by members. Members shall periodically inspect their holsters to make sure they are serviceable and provide the proper security and retention of the handgun.

306.4.3 TACTICAL LIGHTS

Tactical lights may only be installed on a firearm carried on- or off-duty after they have been examined and approved by the Rangemaster. Once the approved tactical lights have been properly installed on any firearm, the member shall qualify with the firearm to ensure proper functionality and sighting of the firearm prior to carrying it.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

306.4.4 OPTICS OR LASER SIGHTS

Optics or laser sights may only be installed on a firearm carried on- or off-duty after they have been examined and approved by the Rangemaster. Any approved sight shall only be installed in strict accordance with manufacturer specifications. Once approved sights have been properly installed on any firearm, the member shall qualify with the firearm to ensure proper functionality and sighting of the firearm prior to carrying it.

Except in an approved training situation, a member may only sight in on a target when the member would otherwise be justified in pointing a firearm at the target.

306.5 SAFE HANDLING, INSPECTION AND STORAGE

Members shall maintain the highest level of safety when handling firearms and shall consider the following:

(a) Members shall not unnecessarily display or handle any firearm.

(b) Members shall be governed by all rules and regulations pertaining to the use of the range and shall obey all orders issued by the Rangemaster. Members shall not dry fire or practice quick draws except under Rangemaster supervision.

(c) Members shall not clean, repair, load or unload a firearm anywhere in the Department, except where clearing barrels are present.

(d) Shotguns or rifles removed from vehicles or the equipment storage room shall be loaded and unloaded in the parking lot and outside of the vehicle, using clearing barrels.

(e) Members shall not place or store any firearm or other weapon on department premises except where the place of storage is locked. No one shall carry firearms into the jail section or any part thereof when securing or processing an arrestee, but shall place all firearms in a secured location. Members providing access to the jail section to persons from outside agencies are responsible for ensuring firearms are not brought into the jail section.

(f) Members shall not use any automatic firearm, heavy caliber rifle, gas or other type of chemical weapon or firearm from the armory, except with approval of a supervisor.

(g) Any firearm authorized by the Department to be carried on- or off-duty that is determined by a member to be malfunctioning or in need of service or repair shall not be carried. It shall be promptly presented to the Department or a Rangemaster approved by the Department for inspection and repair. Any firearm deemed in need of repair or service by the Rangemaster will be immediately removed from service. If the firearm is the member’s primary duty firearm, a replacement firearm will be issued to the member until the duty firearm is serviceable.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

306.5.1 INSPECTION AND STORAGE
Handguns shall be inspected regularly and upon access or possession by another person. Shotguns and rifles shall be inspected at the beginning of the shift by the member to whom the weapon is issued. The member shall ensure that the firearm is carried in the proper condition and loaded with approved ammunition. Inspection of the shotgun and rifle shall be done while standing outside of the patrol vehicle. All firearms shall be pointed in a safe direction or into clearing barrels.

Personally owned firearms may be safely stored in lockers at the end of the shift. Department-owned firearms shall be stored in the appropriate equipment storage room. Handguns may remain loaded if they are secured in an appropriate holster. Shotguns and rifles shall be unloaded in a safe manner outside the building and then stored in the appropriate equipment storage room.

306.5.2 STORAGE AT HOME
Members shall ensure that all firearms and ammunition are locked and secured while in their homes, vehicles or any other area under their control, and in a manner that will keep them inaccessible to children and others who should not have access. Members shall not permit department-issued firearms to be handled by anyone not authorized by the Department to do so. Members should be aware that negligent storage of a firearm could result in civil and criminal liability (Va. Code § 18.2-56.2).

306.5.3 ALCOHOL AND DRUGS
Firearms shall not be carried by any member, either on- or off-duty, who has consumed an amount of an alcoholic beverage, taken any drugs or medication, or taken any combination thereof that would tend to adversely affect the member’s senses or judgment.

306.6 FIREARMS TRAINING AND QUALIFICATIONS
All members who carry a firearm while on-duty are required to successfully complete training quarterly with their duty firearms.

In addition to quarterly training, all members will qualify annually with their duty firearms on the required range course and complete the Virginia Department of Criminal Justice Services (DCJS)-required range course and complete approved in-service training which shall include review of the following (6 VAC 20-30-80):

(a) Nomenclature and care of handgun

(b) Safety (e.g., on the firearms range, on-duty, and off-duty)

(c) Legal responsibilities and liabilities of firearms

(d) Handgun (e.g., handling, firing principles)

(e) Dry firing (e.g., application of basic shooting principles)

(f) Prequalification shooting (150 rounds, minimum)

(g) Virginia Modified Double Action Course for Semi-Automatic Pistols and Revolvers (70 percent minimum qualification required)

(h) Qualification (70 percent minimum required) on one of the following record courses:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1. Modified Tactical Revolver Course
2. Modified Practical Pistol Course
3. Virginia Modified Combat Course I
4. Virginia Modified Combat Course II
5. Virginia Modified Double Action Course for Semi-Automatic Pistols and Revolvers

(i) Familiarization with the shotgun

1. 20 rounds required, shoulder and hip position

(j) Special weapons as required by this department

This annual qualification may substitute for one quarterly training.

The Sheriff shall file any mandated reports with the Director of the DCJS using the DCJS approved forms (6 VAC 20-30-100).

Firearms training and qualification shall be conducted by a certified firearms instructor (6 VAC 20-80-20).

At least annually, all members carrying a firearm should receive practical training designed to simulate field situations including low-light shooting.

306.6.1 NON-CERTIFICATION OR NON-QUALIFICATION

If any member fails to meet minimum standards for firearms training or qualification for any reason, including injury, illness, duty status or scheduling conflict, that member shall submit a memorandum to his/her immediate supervisor prior to the end of the required training or qualification period.

Those who fail to meet minimum standards or qualify on their first shooting attempt shall be provided remedial training and will be subject to the following requirements:

(a) Additional range assignments may be scheduled to assist the member in demonstrating consistent firearm proficiency.

(b) Members shall be given credit for a range training or qualification when obtaining a qualifying score or meeting standards after remedial training.

(c) No range credit will be given for:

1. Unauthorized range make-up.
2. Failure to meet minimum standards or qualify after remedial training.

Members who repeatedly fail to meet minimum standards will be removed from field assignment and may be subject to disciplinary action.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

306.6.2 REQUIREMENTS PRIOR TO CARRYING
Before being authorized to carry any firearm, members will be issued a copy of and be instructed on this policy and the Use of Force Policy. Each member shall acknowledge that the member has been provided access to and has had the opportunity to review and understand these policies. The issuance of and instruction on the policies shall be documented.

306.7 FIREARM DISCHARGE
Except during training or recreational use, any member who discharges a firearm intentionally or unintentionally, on- or off-duty, shall make a verbal report to his/her supervisor as soon as circumstances permit. If the discharge results in injury or death to another person, additional statements and reports shall be made in accordance with the Officer-Involved Shootings and Deaths Policy. If a firearm was discharged as a use of force, the involved member shall adhere to the additional reporting requirements set forth in the Use of Force Policy.

In all other cases, written reports shall be made as follows:

(a) If on-duty at the time of the incident, the member shall file a written report with his/her Division Supervisor or provide a recorded statement to investigators prior to the end of shift, unless otherwise directed.

(b) If off-duty at the time of the incident, the member shall file a written report or provide a recorded statement no later than the end of the next regularly scheduled shift, unless otherwise directed by a supervisor.

306.7.1 DESTRUCTION OF ANIMALS
Members are authorized to use firearms to stop an animal in circumstances where the animal reasonably appears to pose an imminent threat to human safety and alternative methods are not reasonably available or would likely be ineffective.

In circumstances where there is sufficient advance notice that a potentially dangerous animal may be encountered, department members should develop reasonable contingency plans for dealing with the animal (e.g., fire extinguisher, conducted energy device, oleoresin capsicum (OC) spray, animal control officer). Nothing in this policy shall prohibit any member from shooting a dangerous animal if circumstances reasonably dictate that a contingency plan has failed, becomes impractical, or if the animal reasonably appears to pose an imminent threat to human safety.

306.7.2 INJURED ANIMALS
When available, an animal control officer or humane investigator should be summoned to manage injured animals (Va. Code § 3.2-6559).

With the approval of a supervisor, a member may euthanize an animal that is so badly injured that human compassion requires its removal from further suffering and where other dispositions are impractical.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

306.7.3 WARNING AND OTHER SHOTS
Warning shots are prohibited. Generally, shots fired for the purpose of alerting or summoning aid are discouraged and may not be discharged unless the member reasonably believes that they appear necessary, effective and reasonably safe.

306.8 RANGEMASTER DUTIES
The range will be under the exclusive control of the Rangemaster. All members attending will follow the directions of the Rangemaster. The Rangemaster will maintain a roster of all members attending the range and will submit the roster to the Training Supervisor after each range date. Failure of any member to sign in and out with the Rangemaster may result in non-participation or non-qualification.

The range shall remain operational and accessible to department members during hours established by the Department.

The Rangemaster has the responsibility of making periodic inspection, at least once a year, of all duty firearms carried by members of this department to verify proper operation. The Rangemaster has the authority to deem any department-issued or personally owned firearm unfit for service. The member will be responsible for all repairs to his/her personally owned firearm; it will not be returned to service until it has been inspected and approved by the Rangemaster.

The Rangemaster has the responsibility for ensuring each member meets the minimum requirements during training shoots and, on at least a yearly basis, can demonstrate proficiency in the care, cleaning and safety of all firearms the member is authorized to carry.

The Rangemaster shall complete and submit to the Training Supervisor documentation of the training courses provided. Documentation shall include the qualifications of each instructor who provides the training, a description of the training provided and, on a form that has been approved by the Department, a list of each member who completes the training. The Rangemaster should keep accurate records of all training shoots, qualifications, repairs, maintenance or other records as directed by the Training Supervisor.

306.9 FLYING WHILE ARMED
The Transportation Security Administration (TSA) has imposed rules governing law enforcement officers flying armed on commercial aircraft. The following requirements apply to deputies who intend to be armed while flying on a commercial air carrier or flights where screening is conducted (49 CFR 1544.219):

(a) Deputies wishing to fly while armed must be flying in an official capacity, not for vacation or pleasure, and must have a need to have the firearm accessible, as determined by the Department based on the law and published TSA rules.

(b) Deputies must carry their Madison County Sheriff's Office identification card, bearing the deputy’s name, a full-face photograph, identification number, the deputy’s signature and the signature of the Sheriff or the official seal of the Department and must present this identification to airline officials when requested. The deputy should

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

also carry the standard photo identification needed for passenger screening by airline and TSA officials (e.g., driver's license, passport).

(c) The Madison County Sheriff's Office must submit a National Law Enforcement Telecommunications System (NLETS) message prior to the deputy's travel. If approved, TSA will send the Madison County Sheriff's Office an NLETS message containing a unique alphanumeric identifier. The deputy must present the message on the day of travel to airport personnel as authorization to travel while armed.

(d) An official letter signed by the Sheriff authorizing armed travel may also accompany the deputy. The letter should outline the deputy's need to fly armed, detail his/her itinerary, and include that the deputy has completed the mandatory TSA training for a law enforcement officer flying while armed.

(e) Deputies must have completed the mandated TSA security training covering deputies flying while armed. The training shall be given by the department-appointed instructor.

(f) It is the deputy's responsibility to notify the air carrier in advance of the intended armed travel. This notification should be accomplished by early check-in at the carrier's check-in counter.

(g) Any deputy flying while armed should discreetly contact the flight crew prior to take-off and notify them of his/her assigned seat.

(h) Discretion must be used to avoid alarming passengers or crew by displaying a firearm. The deputy must keep the firearm concealed on his/her person at all times. Firearms are not permitted in carry-on luggage and may not be stored in an overhead compartment.

(i) Deputies should try to resolve any problems through the flight captain, ground security manager, TSA representative or other management representative of the air carrier.

(j) Deputies shall not consume alcoholic beverages while aboard an aircraft, or within eight hours prior to boarding an aircraft.

306.10 CARRYING FIREARMS OUT OF STATE

Qualified, active, full-time deputies of this department are authorized to carry a concealed firearm in all other states subject to the following conditions (18 USC § 926B):

(a) The deputy shall carry his/her Madison County Sheriff's Office identification card whenever carrying such firearm.

(b) The deputy may not be the subject of any current disciplinary action.

(c) The deputy may not be under the influence of alcohol or any other intoxicating or hallucinatory drug.

(d) The deputy will remain subject to this and all other department policies (including qualifying and training).

Deputies are cautioned that individual states may enact local regulations that permit private persons or entities to prohibit or restrict the possession of concealed firearms on their property, or that prohibit or restrict the possession of firearms on any state or local government property,

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

installation, building, base or park. Federal authority may not shield a deputy from arrest and prosecution in such locally restricted areas.

Active law enforcement officers from other states are subject to all requirements set forth in 18 USC § 926B.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Vehicle Pursuits

307.1 PURPOSE AND SCOPE

This policy provides guidelines for vehicle pursuits in order to protect the safety of involved deputies, the public and fleeing suspects.

307.1.1 DEFINITIONS

Definitions related to this policy include:

Blocking or vehicle intercept - A slow-speed coordinated maneuver where two or more pursuing vehicles simultaneously intercept and block the movement of a suspect vehicle, the driver of which may be unaware of the impending enforcement stop. The goal is containment and preventing a pursuit. Blocking is not a moving or stationary road block.

Boxing-in - A tactic designed to stop a suspect's vehicle by surrounding it with law enforcement vehicles and then slowing all vehicles to a stop.

Due regard - to give fair consideration and sufficient attention to all of the facts such that a reasonably careful man performing similar duties and under the same circumstances would act in the same manner.

Ramming - The deliberate act of contacting a suspect's vehicle with another law enforcement vehicle to functionally damage or otherwise force the suspect's vehicle to stop.

Roadblocks - A tactic designed to stop a suspect's vehicle by intentionally placing a law enforcement vehicle or other immovable object in the path of the suspect's vehicle.

Terminate - To discontinue a pursuit or stop chasing fleeing vehicles.

Tire deflation device - A device designed to puncture the tires of the pursued vehicle.

Trail - Following the path of the pursuit at a safe speed while obeying all traffic laws and without activating emergency equipment. If the pursuit is at a slow rate of speed, the trailing vehicle will maintain sufficient distance from the pursuit vehicles so as to clearly indicate an absence of participation in the pursuit.

Vehicle pursuit - An event involving one or more law enforcement officers attempting to apprehend a suspect, who is attempting to avoid arrest while operating a vehicle by using high-speed driving or other evasive tactics, such as driving off a highway, turning suddenly or driving in a legal manner but willfully failing to yield to a deputy's emergency signal to stop.

307.2 POLICY

It is the policy of this department to weigh the importance of apprehending suspects who unlawfully flee from law enforcement against the risks associated with vehicle pursuits.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

307.3 DEPUTY RESPONSIBILITIES

Vehicle pursuits shall only be conducted using authorized sheriff's department emergency vehicles that are equipped with emergency lighting and sirens as required by law (Va. Code § 46.2-1022; Va. Code § 46.2-1061).

Deputies shall drive with due regard for the safety of all persons and property. However, deputies may, when in pursuit of a suspect and provided there is no unreasonable risk to persons and property (Va. Code § 46.2-920):

(a) Disregard speed limits, while having due regard for safety of persons and property.

(b) Proceed past any steady or flashing red signal, traffic light, stop sign, or device indicating moving traffic shall stop if the speed of the vehicle is sufficiently reduced to enable it to pass a signal, traffic light, or device with due regard to the safety of persons and property

(c) Disregard regulations governing a direction of movement of vehicles turning in specified directions so long as the operator does not endanger life or property.

(d) Park or stop where it is otherwise prohibited.

(e) Pass or overtake, with due regard to the safety of persons and property, another vehicle at any intersection.

(f) Pass or overtake with due regard to the safety of persons and property, while en route to an emergency, stopped or slow-moving vehicles, by going to the left of the stopped or slow-moving vehicle either in a no-passing zone or by crossing the highway centerline.

(g) Pass or overtake with due regard to the safety of persons and property, while en route to an emergency, stopped or slow-moving vehicles, by going off the paved or main traveled portion of the roadway on the right. Vehicles exempted in this instance will not be required to sound a siren or any device to give automatically intermittent signals.

307.3.1 WHEN TO INITIATE A PURSUIT

Deputies are authorized to initiate a pursuit when it is reasonable to believe that a suspect, who has been given an appropriate signal to stop by a law enforcement officer, is attempting to evade arrest or detention by fleeing in a vehicle.

Factors that shall be considered, both individually and collectively, when deciding to initiate or continue a pursuit include, but are not limited to:

(a) The seriousness of the known or reasonably suspected crime and its relationship to community safety.

(b) The importance of protecting the public and balancing the known or reasonably suspected offense and the apparent need for immediate capture against the risks to deputies, innocent motorists and others.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) The safety of the public in the area of the pursuit, including the type of area, time of day, the amount of vehicular and pedestrian traffic (e.g., school zones) and the speed of the pursuit relative to these factors.

(d) The pursuing deputies' familiarity with the area of the pursuit, the quality of radio communications between the pursuing vehicles and dispatcher/supervisor, and the driving capabilities of the pursuing deputies under the conditions of the pursuit.

(e) Whether weather, traffic and road conditions unreasonably increase the danger of the pursuit when weighed against the risks resulting from the suspect's escape.

(f) Whether the identity of the suspect has been verified and whether there is comparatively minimal risk in allowing the suspect to be apprehended at a later time.

(g) The performance capabilities of the vehicles used in the pursuit in relation to the speed and other conditions of the pursuit.

(h) Emergency lighting and siren limitations on unmarked sheriff's department vehicles that may reduce visibility of the vehicle, such as visor or dash-mounted lights, concealable or temporary emergency lighting equipment and concealed or obstructed siren positioning.

(i) Vehicle speeds.

(j) Other persons in or on the pursued vehicle (e.g., passengers, co-offenders and hostages).

(k) The availability of other resources, such as air support assistance.

(l) Whether the pursuing vehicle is carrying passengers other than on-duty sheriff's deputies. Pursuits should not be undertaken with an arrestee in the pursuit vehicle unless exigent circumstances exist, and then only after the need to apprehend the suspect is weighed against the safety of the arrestee in transport. A vehicle containing more than a single arrestee should not be involved in a pursuit.

307.3.2 WHEN TO TERMINATE A PURSUIT

Pursuits should be terminated whenever the totality of objective circumstances known or which reasonably ought to be known to the deputy or supervisor during the pursuit indicates that the present risks of continuing the pursuit reasonably appear to outweigh the risks resulting from the suspect's escape.

When a supervisor directs the pursuit to be terminated, deputies will immediately terminate the pursuit.

The factors listed in this policy on when to initiate a pursuit will apply equally to the decision to terminate a pursuit. Deputies and supervisors must objectively and continuously weigh the seriousness of the offense against the potential danger to innocent motorists, themselves and the public when electing to continue a pursuit.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

In addition to the factors that govern when to initiate a pursuit, other factors should be considered in deciding whether to terminate a pursuit, including:

(a) The distance between the pursuing vehicle and the fleeing vehicle is so great that further pursuit would be futile or require the pursuit to continue for an unreasonable time or distance.

(b) The pursued vehicle's location is no longer definitely known.

(c) The pursuing vehicle sustains damage or a mechanical failure that renders it unsafe to drive.

(d) The pursuing vehicle's emergency lighting equipment or siren becomes partially or completely inoperable.

(e) Hazards posed to uninvolved bystanders or motorists.

(f) The danger that the continued pursuit poses to the public, the deputies or the suspect, balanced against the risk of allowing the suspect to remain at large.

(g) The identity of the suspect is known and it does not reasonably appear that the need for immediate capture outweighs the risks associated with continuing the pursuit.

(h) Extended pursuits of violators for misdemeanors not involving violence or weapons (independent of the pursuit) are generally discouraged.

307.4 PURSUIT VEHICLES

When involved in a pursuit, unmarked sheriff's department emergency vehicles should be replaced by marked emergency vehicles whenever practicable.

Vehicle pursuits should be limited to three sheriff's department emergency vehicles (two pursuit vehicles and the supervisor vehicle). However, the number of vehicles involved will vary with the circumstances.

A deputy or supervisor may request that additional vehicles join a pursuit if, after assessing the factors outlined above, it appears that the number of deputies involved would be insufficient to safely arrest the number of suspects. All other deputies shall stay out of the pursuit but should remain alert to its progress and location. Any deputy who drops out of a pursuit may then, if necessary, proceed to the pursuit termination point at legal speeds, following the appropriate rules of the road.

307.4.1 MOTORCYCLES

When involved in a pursuit, sheriff's department motorcycles should be replaced by marked emergency vehicles as soon as practicable.

307.4.2 VEHICLES WITHOUT EMERGENCY EQUIPMENT

Deputies operating vehicles not equipped with emergency lights and siren are prohibited from initiating or joining in any pursuit. Deputies in such vehicles may provide support to pursuing

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

vehicles as long as the vehicle is operated in compliance with all traffic laws. Those deputies should discontinue such support immediately upon arrival of a sufficient number of authorized emergency sheriff's department vehicles or any air support.

307.4.3 PRIMARY PURSUIT VEHICLE RESPONSIBILITIES

The initial pursuing deputy will be designated as the primary pursuit vehicle and will be responsible for the conduct of the pursuit unless he/she is unable to remain reasonably close to the suspect's vehicle. The primary responsibility of the deputy initiating the pursuit is the apprehension of the suspect without unreasonable danger to him/herself or others.

The primary pursuing deputy should notify the dispatcher, commencing with a request for priority radio traffic, that a vehicle pursuit has been initiated, and as soon as practicable provide information including, but not limited to:

(a) The location, direction of travel and estimated speed of the suspect's vehicle.

(b) The description of the suspect's vehicle including the license plate number, if known.

(c) The reason for the pursuit.

(d) The use of firearms, threat of force, violence, injuries, hostages or other unusual hazards.

(e) The number of occupants and identity or description.

(f) The weather, road and traffic conditions.

(g) The need for any additional resources or equipment.

(h) The identity of other law enforcement agencies involved in the pursuit.

Until relieved by a supervisor or a secondary pursuing deputy, the deputy in the primary pursuit vehicle shall be responsible for broadcasting the progress of the pursuit. Unless circumstances reasonably indicate otherwise, the primary pursuing deputy should, as soon as practicable, relinquish the responsibility of broadcasting the progress of the pursuit to a deputy in a secondary pursuit vehicle or to air support joining the pursuit to minimize distractions and allow the primary pursuing deputy to concentrate foremost on safe pursuit tactics.

307.4.4 SECONDARY PURSUIT VEHICLE RESPONSIBILITIES

The second deputy in the pursuit will be designated as the secondary pursuit vehicle and is responsible for:

(a) Immediately notifying the dispatcher of his/her entry into the pursuit.

(b) Remaining a safe distance behind the primary pursuit vehicle unless directed to assume the role of primary pursuit vehicle or if the primary pursuit vehicle is unable to continue the pursuit.

(c) Broadcasting information that the primary pursuing deputy is unable to provide.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Broadcasting the progress of the pursuit, updating known or critical information and providing changes in the pursuit, unless the situation indicates otherwise.

(e) Identifying the need for additional resources or equipment as appropriate.

(f) Serving as backup to the primary pursuing deputy once the suspect has been stopped.

307.5 PURSUIT DRIVING

The decision to use specific driving tactics requires the same assessment of the factors the deputy considered when determining whether to initiate and/or terminate a pursuit. The following are tactics for deputies who are involved in the pursuit:

(a) Deputies, considering their driving skills and vehicle performance capabilities, will space themselves from other involved vehicles such that they are able to see and avoid hazards or react safely to unusual maneuvers by the fleeing vehicle.

(b) Because intersections can present increased risks, the following tactics should be considered:

1. Available deputies not directly involved in the pursuit may proceed safely to controlled intersections ahead of the pursuit in an effort to warn cross traffic.
2. Pursuing deputies should exercise due caution and slow down as may be necessary when proceeding through controlled intersections.

(c) As a general rule, deputies should not pursue a vehicle driving the wrong direction on a roadway, highway or freeway. In the event the pursued vehicle does so, the following tactics should be considered:

1. Request assistance from available air support.
2. Maintain visual contact with the pursued vehicle by paralleling the vehicle while driving on the correct side of the roadway.
3. Request other deputies to observe exits available to the suspect.

(d) Notify the Virginia State Police or other law enforcement agency if it appears that the pursuit may enter its jurisdiction.

(e) Deputies involved in a pursuit should not attempt to pass other pursuing vehicles unless the situation indicates otherwise or they are requested to do so by the pursuing deputy and with a clear understanding of the maneuver process between the involved deputies.

307.5.1 PURSUIT TRAILING

In the event that initial pursuing deputies relinquish control of the pursuit to another agency, the initial deputies may, with the permission of a supervisor, trail the pursuit to the termination point in order to provide information and assistance for the arrest of the suspect and reporting the incident.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

307.5.2 AIR SUPPORT ASSISTANCE

When available, air support assistance should be requested. Once the air support crew has established visual contact with the pursued vehicle, they should assume communication control over the pursuit. The primary and secondary ground pursuit vehicles, or involved supervisor, will maintain operational control but should consider whether the participation of air support warrants their continued close proximity and/or involvement in the pursuit.

The air support crew should coordinate the activities of resources on the ground, report progress of the pursuit, and provide deputies and supervisors with details of upcoming traffic congestion, road hazards or other pertinent information to evaluate whether to continue the pursuit. If deputies on the ground are not within visual contact of the pursued vehicle and the air support crew determines that it is unsafe to continue the pursuit, the air support crew should recommend terminating the pursuit.

307.5.3 DEPUTIES NOT INVOLVED IN THE PURSUIT

Deputies who are not involved in the pursuit should remain in their assigned areas, should not parallel the pursuit route and should not become involved with the pursuit unless directed otherwise by a supervisor. Uninvolved deputies are authorized to use emergency equipment at intersections along the pursuit path to clear intersections of vehicular and pedestrian traffic to protect the public. Those deputies should attempt to place their vehicles in locations that provide some safety or an escape route in the event of an unintended collision or if the suspect intentionally tries to ram the sheriff's department vehicle.

Non-pursuing members needed at the pursuit termination point should respond in a non-emergency manner, observing the rules of the road.

The primary pursuit vehicle, secondary pursuit vehicle and supervisor vehicle should be the only vehicles operating under emergency conditions (emergency lights and siren) unless other deputies are assigned to the pursuit.

307.6 SUPERVISORY CONTROL AND RESPONSIBILITIES

Available supervisory and management control will be exercised over all vehicle pursuits involving deputies from this department.

The field supervisor of the deputy initiating the pursuit, or if unavailable, the nearest field supervisor, will be responsible for:

(a) Immediately notifying involved deputies and the dispatcher of supervisory presence and ascertaining all reasonably available information to continuously assess the situation and risk factors associated with the pursuit. This is to ensure that the pursuit is conducted within established department guidelines.

(b) Engaging in the pursuit, when appropriate, to provide on-scene supervision.

(c) Exercising management and control of the pursuit even if not engaged in it.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Ensuring that no more than the required law enforcement vehicles are involved in the pursuit under the guidelines set forth in this policy.

(e) Directing that the pursuit be terminated if, in his/her judgment, it is not justified to continue the pursuit under the guidelines of this policy.

(f) Ensuring that assistance from air support, canines or additional resources is requested, if available and appropriate.

(g) Ensuring that the proper radio channel is being used.

(h) Ensuring that the Shift Supervisor is notified of the pursuit, as soon as practicable.

(i) Ensuring the notification and/or coordination of outside agencies if the pursuit either leaves or is likely to leave the jurisdiction of this department.

(j) Controlling and managing Madison County Sheriff's Office deputies when a pursuit enters another jurisdiction.

(k) Preparing a post-pursuit review and documentation of the pursuit as required.

307.6.1 SHIFT SUPERVISOR RESPONSIBILITIES

Upon becoming aware that a pursuit has been initiated, the Shift Supervisor should monitor and continually assess the situation and ensure the pursuit is conducted within the guidelines and requirements of this policy. The Shift Supervisor has the final responsibility for the coordination, control and termination of a vehicle pursuit and shall be in overall command.

The Shift Supervisor shall review all pertinent reports for content and forward them to the Division Supervisor.

307.7 THE DISPATCH CENTER

If the pursuit is confined within the County limits, radio communications will be conducted on the primary channel unless instructed otherwise by a supervisor or dispatcher. If the pursuit leaves the jurisdiction of this department or such is imminent, involved deputies should, whenever available, switch radio communications to a tactical or emergency channel most accessible by participating agencies.

307.7.1 RESPONSIBILITIES

Upon notification or becoming aware that a pursuit has been initiated, the dispatcher is responsible for:

(a) Clearing the radio channel of non-emergency traffic.

(b) Coordinating pursuit communications of the involved deputies.

(c) Broadcasting pursuit updates as well as other pertinent information as necessary.

(d) Ensuring that a field supervisor is notified of the pursuit.

(e) Notifying and coordinating with other involved or affected agencies as practicable.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(f) Notifying the Shift Supervisor as soon as practicable.

(g) Assigning an incident number and logging all pursuit activities.

307.8 LOSS OF PURSUED VEHICLE

When the pursued vehicle is lost, the involved deputies should broadcast pertinent information to assist other deputies in locating the vehicle. The primary pursuing deputy or supervisor will be responsible for coordinating any further search for either the pursued vehicle or suspects fleeing on foot.

307.9 INTERJURISDICTIONAL CONSIDERATIONS

When a pursuit enters another agency's jurisdiction, the primary pursuing deputy or supervisor, taking into consideration the distance traveled, unfamiliarity with the area and other pertinent facts, should determine whether to request the other agency to assume the pursuit.

Unless entry into another jurisdiction is expected to be brief, it is generally recommended that the primary pursuing deputy or supervisor ensure that notification is provided to each outside jurisdiction into which the pursuit is reasonably expected to enter, regardless of whether the jurisdiction is expected to assist.

307.9.1 ASSUMPTION OF PURSUIT BY ANOTHER AGENCY

Deputies will relinquish control of the pursuit when another agency has assumed the pursuit, unless the continued assistance of the Madison County Sheriff's Office is requested by the agency assuming the pursuit. Upon relinquishing control of the pursuit, the involved deputies may proceed, with supervisory approval, to the termination point of the pursuit to assist in the investigation. The supervisor should coordinate such assistance with the assuming agency and obtain any information that is necessary for any reports.

The roles and responsibilities of deputies at the termination point of a pursuit initiated by this department shall be coordinated with appropriate consideration of the needs of the agency assuming the pursuit.

Notification of a pursuit in progress should not be construed as a request to join the pursuit. Requests to or from another agency to assume a pursuit should be specific. Because of communication limitations between local law enforcement agencies, a request for another agency’s assistance will mean that its personnel will assume responsibility for the pursuit. For the same reasons, when a pursuit leaves another jurisdiction and a request for assistance is made to this department, the other agency should relinquish control.

307.9.2 PURSUITS EXTENDING INTO THIS JURISDICTION

The agency that initiates a pursuit shall be responsible for conducting the pursuit. Deputies from this department should not join a pursuit unless specifically requested to do so by the pursuing agency and with approval from a supervisor. The exception to this is when a single vehicle from the initiating agency is in pursuit. Under this circumstance, a deputy from this department may, with

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

supervisor approval, immediately join the pursuit until sufficient vehicles from the initiating agency join the pursuit or until additional information is provided allowing withdrawal from the pursuit.

When a request is made for this department to assist or take over a pursuit that has entered the jurisdiction of the Madison County Sheriff's Office, the supervisor should consider:

(a) The public’s safety within this jurisdiction.

(b) The safety of the pursuing deputies.

(c) Whether the circumstances are serious enough to continue the pursuit.

(d) Whether there is adequate staffing to continue the pursuit.

(e) The ability to maintain the pursuit.

As soon as practicable, a supervisor or the Shift Supervisor should review a request for assistance from another agency. The Shift Supervisor or supervisor, after considering the above factors, may decline to assist in or assume the other agency’s pursuit.

Assistance to a pursuing agency by deputies of this department will conclude at the County limits, provided that the pursuing agency has sufficient assistance from other sources. Ongoing participation from this department may continue only until sufficient assistance is present.

In the event that the termination point of a pursuit from another agency is within this jurisdiction, deputies shall provide appropriate assistance including, but not limited to, scene control, coordination and completion of supplemental reports and any other assistance requested or needed.

307.10 PURSUIT INTERVENTION

Pursuit intervention is an attempt to stop the suspect's ability to continue to flee in a vehicle through tactical application of technology, tire deflation devices, blocking or vehicle intercept, boxing-in, ramming or roadblock procedures.

307.10.1 WHEN USE IS AUTHORIZED

Whenever practicable, a deputy shall seek approval from a supervisor before employing any intervention to stop the pursued vehicle. In deciding whether to use intervention tactics, deputies/ supervisors should balance the risk of allowing the pursuit to continue with the potential hazards arising from the use of each tactic to the public, the deputies and persons in or on the pursued vehicle. With this in mind, the decision to use any intervention tactic should be reasonable in light of the circumstances apparent to the deputy at the time of the decision.

307.10.2 USE OF FIREARMS

The use of firearms to disable a pursued vehicle is not generally an effective tactic and involves all the dangers associated with discharging firearms. Deputies should not utilize firearms during an ongoing pursuit unless the conditions and circumstances meet the requirements authorizing the use of deadly force. Nothing in this section shall be construed to prohibit any deputy from using a firearm to stop a suspect from using a vehicle as a deadly weapon.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

307.10.3 INTERVENTION STANDARDS

Any intervention tactic, depending upon the conditions and circumstances under which it is used, may present dangers to the deputies, the public or anyone in or on the vehicle being pursued. Certain applications of intervention tactics may be construed to be a use of force, including deadly force, and are subject to policies guiding such use. Deputies shall consider these facts and requirements prior to deciding how, when, where and if an intervention tactic should be employed.

(a) Blocking or vehicle intercept should only be considered in cases involving felony suspects or impaired drivers who pose a threat to the public's safety, and when deputies reasonably believe that attempting a conventional enforcement stop will likely result in the driver attempting to flee in the vehicle. Because of the potential risks involved, this intervention tactic should only be employed by properly trained deputies and after giving consideration to the following:

1. The need to immediately stop the suspect vehicle or prevent it from leaving substantially outweighs the risk of injury or death to occupants of the suspect vehicle, deputies or others.
2. All other reasonable intervention tactics have failed or reasonably appear ineffective.
3. Employing the blocking or vehicle intercept maneuver does not unreasonably increase the risk of danger to those involved or the public.
4. The suspect vehicle is stopped or traveling at a low speed.
5. Only law enforcement vehicles should be used in this tactic.

(b) Ramming a fleeing vehicle should be done only after other reasonable tactical means at the deputy's disposal have been exhausted or would not be effective, and immediate control is necessary. Ramming should be reserved for situations where there does not appear to be another reasonable alternative method. If there does not reasonably appear to be a present or immediately foreseeable serious threat to the public, the use of ramming is not authorized. When ramming is used as a means to stop a fleeing vehicle, the following factors should be present:

1. The suspect is an actual or suspected felon, who reasonably appears to represent a serious threat to the public if not apprehended.
2. The suspect is driving with willful or wanton disregard for the safety of other persons or is driving in a reckless and life-endangering manner or using the vehicle as a weapon.

(c) Boxing-in a suspect vehicle should only be attempted upon approval by a supervisor. The use of such a tactic must be carefully coordinated with all involved vehicles, taking into consideration the circumstances and conditions apparent at the time, as well as the potential risk of injury to deputies, the public and occupants of the pursued vehicle. Deputies and supervisors should weigh the potential consequences against the need to immediately stop the vehicle.

(d) Tire deflation devices should be deployed only after notification of pursuing deputies and the supervisor of the intent and location of the intended deployment, and in a manner that:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1. Should reasonably only affect the pursued vehicle.
2. Provides the deploying deputy adequate cover and escape from intentional or unintentional exposure to the approaching vehicle.
3. Takes into account the limitations of such devices as well as the potential risk to deputies, the public and occupants of the pursued vehicle.
4. Takes into account whether the pursued vehicle is a motorcycle, a vehicle transporting hazardous materials or a school bus transporting children.

(e) Because roadblocks involve a potential for serious injury or death to occupants of the pursued vehicle if the suspect does not stop, the intentional placement of roadblocks in the direct path of a pursued vehicle is generally discouraged and should not be deployed without prior approval of a supervisor. If roadblocks are deployed, it should only be done under extraordinary conditions when all other reasonable intervention tactics have failed or reasonably appear ineffective and the need to immediately stop the pursued vehicle substantially outweighs the risks of injury or death to occupants of the pursued vehicle, deputies or the public.

307.11 CAPTURE OF SUSPECTS

Proper self-discipline and sound professional judgment are the keys to a successful conclusion of a pursuit and apprehension of evading suspects. Deputies shall use only that amount of force that reasonably appears necessary given the facts and circumstances perceived by the deputy at the time of the event to accomplish a legitimate law enforcement purpose.

Unless relieved by a supervisor, the primary pursuing deputy should coordinate efforts to apprehend the suspect following the pursuit. Deputies should consider the safety of the public and the involved deputies when formulating plans for setting up perimeters or for containing and capturing the suspect.

307.12 REPORTING REQUIREMENTS

All appropriate reports shall be completed to comply with appropriate laws and policies or procedures.

(a) The primary pursuing deputy shall complete appropriate crime/arrest reports.

(b) The primary pursuing deputy or supervisor shall complete the appropriate pursuit report.

(c) After first obtaining the available information, the involved, or if unavailable, on-duty field supervisor shall promptly complete a supervisor's log or interoffice memorandum, briefly summarizing the pursuit to the Sheriff or the authorized designee. This log or memorandum should include, at a minimum:

1. Date and time of the pursuit.
2. Initial reason and circumstances surrounding the pursuit.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

3. Length of pursuit in distance and time, including the starting and termination points.
4. Involved vehicles and deputies.
5. Alleged offenses.
6. Whether a suspect was apprehended, as well as the means and methods used.
    (a) Any use of force shall be reported and documented in compliance with the Use of Force Policy.
7. Arrestee information, if applicable.
8. Any injuries and/or medical treatment.
9. Any property or equipment damage.
10. Name of supervisor at the scene or who handled the incident.
11. A preliminary determination that the pursuit appears to be in compliance with this policy or that additional review and/or follow-up is warranted.

(d) After receiving copies of reports, logs and other pertinent information, the Sheriff or the authorized designee shall conduct or assign the completion of a post-pursuit review, as appropriate.

(e) Annually, the Sheriff should direct a documented review and analysis of department vehicle pursuits to minimally include policy suitability, policy compliance and training needs.

307.13 REGULAR AND PERIODIC PURSUIT TRAINING

In addition to initial and supplementary training on pursuits, all deputies will participate, no less than annually, in regular and periodic training addressing this policy and the importance of vehicle safety and protecting the public. Training will include recognition of the need to balance the known offense and the need for immediate capture against the risks to deputies and others.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Foot Pursuits

308.1 PURPOSE AND SCOPE

This policy provides guidelines to assist deputies in making the decision to initiate or continue the pursuit of suspects on foot.

308.2 POLICY

It is the policy of this department that deputies, when deciding to initiate or continue a foot pursuit, continuously balance the objective of apprehending the suspect with the risk and potential for injury to department members, the public or the suspect.

Deputies are expected to act reasonably, based on the totality of the circumstances.

308.3 DECISION TO PURSUE

The safety of department members and the public should be the primary consideration when determining whether a foot pursuit should be initiated or continued. Deputies must be mindful that immediate apprehension of a suspect is rarely more important than the safety of the public and department members.

Deputies may be justified in initiating a foot pursuit of any individual that the deputy reasonably believes is about to engage in, is engaging in or has engaged in criminal activity. The decision to initiate or continue such a foot pursuit, however, must be continuously re-evaluated in light of the circumstances presented at the time.

Mere flight by a person who is not suspected of criminal activity alone shall not serve as justification for engaging in an extended foot pursuit without the development of reasonable suspicion regarding the individual's involvement in criminal activity or being wanted by law enforcement.

Deciding to initiate or continue a foot pursuit is a decision that a deputy must make quickly and under unpredictable and dynamic circumstances. It is recognized that foot pursuits may place department members and the public at significant risk.

If circumstances permit, surveillance and containment are generally the safest tactics for apprehending fleeing persons. In deciding whether to initiate or continue a foot pursuit, a deputy should continuously consider reasonable alternatives to a foot pursuit based upon the circumstances and resources available, such as:

(a) Containment of the area.

(b) Saturation of the area with law enforcement personnel, including assistance from other agencies.

(c) A canine search.

(d) Thermal imaging or other sensing technology.

(e) Air support.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(f) Apprehension at another time when the identity of the suspect is known or there is information available that would likely allow for later apprehension, and the need to immediately apprehend the suspect does not reasonably appear to outweigh the risk of continuing the foot pursuit.

308.4 GENERAL GUIDELINES

When reasonably practicable, deputies should consider alternatives to engaging in or continuing a foot pursuit when:

(a) Directed by a supervisor to terminate the foot pursuit; such an order shall be considered mandatory.

(b) The deputy is acting alone.

(c) Two or more deputies become separated, lose visual contact with one another or obstacles separate them to the degree that they cannot immediately assist each other should a confrontation take place. In such circumstances, it is generally recommended that a single deputy keep the suspect in sight from a safe distance and coordinate the containment effort.

(d) The deputy is unsure of his/her location and direction of travel.

(e) The deputy is pursuing multiple suspects and it is not reasonable to believe that the deputy would be able to control the suspects should a confrontation occur.

(f) The physical condition of the deputy renders him/her incapable of controlling the suspect if apprehended.

(g) The deputy loses radio contact with the dispatcher or with assisting or backup deputies.

(h) The suspect enters a building, structure, confined space, isolated area or dense or difficult terrain, and there are insufficient deputies to provide backup and containment. The primary deputy should consider discontinuing the foot pursuit and coordinating containment pending the arrival of sufficient resources.

(i) The deputy becomes aware of unanticipated or unforeseen circumstances that unreasonably increase the risk to deputies or the public.

(j) The deputy reasonably believes that the danger to the pursuing deputies or public outweighs the objective of immediate apprehension.

(k) The deputy loses possession of his/her firearm or other essential equipment.

(l) The deputy or a third party is injured during the foot pursuit, requiring immediate assistance, and there are no other emergency personnel available to render assistance.

(m) The suspect’s location is no longer known.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(n) The identity of the suspect is established or other information exists that will allow for the suspect's apprehension at a later time, and it reasonably appears that there is no immediate threat to department members or the public if the suspect is not immediately apprehended.

(o) The deputy's ability to safely continue the foot pursuit is impaired by inclement weather, darkness or other environmental conditions.

308.5 RESPONSIBILITIES IN FOOT PURSUITS

308.5.1 INITIATING DEPUTY RESPONSIBILITIES

Unless relieved by another deputy or a supervisor, the initiating deputy shall be responsible for coordinating the progress of the pursuit and containment. When acting alone and when practicable, the initiating deputy should not attempt to overtake and confront the suspect but should attempt to keep the suspect in sight until sufficient deputies are present to safely apprehend the suspect.

Early communication of available information from the involved deputies is essential so that adequate resources can be coordinated and deployed to bring a foot pursuit to a safe conclusion. Deputies initiating a foot pursuit should, at a minimum, broadcast the following information as soon as it becomes practicable and available:

(a) Location and direction of travel

(b) Call sign identifier

(c) Reason for the foot pursuit, such as the crime classification

(d) Number of suspects and description, to include name if known

(e) Whether the suspect is known or believed to be armed with a dangerous weapon

Deputies should be mindful that radio transmissions made while running may be difficult to understand and may need to be repeated.

Absent extenuating circumstances, any deputy unable to promptly and effectively broadcast this information should terminate the foot pursuit. If the foot pursuit is discontinued for any reason, immediate efforts for containment should be established and alternatives considered based upon the circumstances and available resources.

When a foot pursuit terminates, the deputy will notify the dispatcher of his/her location and the status of the foot pursuit termination (e.g., suspect in custody, lost sight of suspect), and will direct further actions as reasonably appear necessary, to include requesting medical aid as needed for deputies, suspects or members of the public.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

308.5.2 ASSISTING DEPUTY RESPONSIBILITIES

Whenever any deputy announces that he/she is engaged in a foot pursuit, all other deputies should minimize nonessential radio traffic to permit the involved deputies maximum access to the radio frequency.

308.5.3 SUPERVISOR RESPONSIBILITIES

Upon becoming aware of a foot pursuit, the supervisor shall make every reasonable effort to ascertain sufficient information to direct responding resources and to take command, control and coordination of the foot pursuit. The supervisor should respond to the area whenever possible; the supervisor does not, however, need to be physically present to exercise control over the foot pursuit. The supervisor shall continuously assess the situation in order to ensure the foot pursuit is conducted within established department guidelines.

The supervisor shall terminate the foot pursuit when the danger to pursuing deputies or the public appears to unreasonably outweigh the objective of immediate apprehension of the suspect.

Upon apprehension of the suspect, the supervisor shall promptly proceed to the termination point to direct the post-foot pursuit activity.

308.5.4 THE DISPATCH CENTER RESPONSIBILITIES

Upon notification or becoming aware that a foot pursuit is in progress, the dispatcher is responsible for:

(a) Clearing the radio channel of non-emergency traffic.

(b) Coordinating pursuit communications of the involved deputies.

(c) Broadcasting pursuit updates as well as other pertinent information as necessary.

(d) Ensuring that a field supervisor is notified of the foot pursuit.

(e) Notifying and coordinating with other involved or affected agencies as practicable.

(f) Notifying the Shift Supervisor as soon as practicable.

(g) Assigning an incident number and logging all pursuit activities.

308.6 REPORTING REQUIREMENTS

The initiating deputy shall complete appropriate crime/arrest reports documenting, at a minimum:

(a) Date and time of the foot pursuit.

(b) Initial reason and circumstances surrounding the foot pursuit.

(c) Course and approximate distance of the foot pursuit.

(d) Alleged offenses.

(e) Involved vehicles and deputies.

(f) Whether a suspect was apprehended as well as the means and methods used.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1. Any use of force shall be reported and documented in compliance with the Use of Force Policy.

(g) Arrestee information, if applicable.

(h) Any injuries and/or medical treatment.

(i) Any property or equipment damage.

(j) Name of the supervisor at the scene or who handled the incident.

Assisting deputies taking an active role in the apprehension of the suspect shall complete supplemental reports as necessary or as directed.

- The supervisor reviewing the report will make a preliminary determination that the pursuit appears to be in compliance with this policy or that additional review and/or follow-up is warranted.

In any case in which a suspect is not apprehended and there is insufficient information to support further investigation, a supervisor may authorize that the initiating deputy need not complete a formal report.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Deputy Response to Calls

309.1 PURPOSE AND SCOPE

This policy provides deputies with guidelines for the safe and appropriate vehicular response to emergency and non-emergency incidents or requests for assistance, whether these are dispatched or self-initiated.

309.1.1 DEFINITIONS

Due regard - to give fair consideration and sufficient attention to all of the facts such that a reasonably careful man performing similar duties and under the same circumstances would act in the same manner.

309.2 POLICY

It is the policy of this department to appropriately respond to emergency and non-emergency calls for service or requests for assistance, whether these are dispatched or self-initiated.

309.3 RESPONSE TO CALLS

Deputies responding to non-emergency calls shall proceed accordingly, unless they are sent or redirected to a higher priority call, and shall obey all traffic laws.

309.3.1 EMERGENCY CALLS

Deputies responding to an emergency call shall proceed immediately as appropriate and shall continuously operate the emergency vehicle lighting and siren as required by law (Va. Code § 46.2-920).

Deputies should only respond to a call as an emergency response when so dispatched or when circumstances reasonably indicate an emergency response is required. This includes, but is not limited to:

(a) When in pursuit or apprehending a violator or suspected violator.

(b) When responding to a reported emergency involving possible personal injury, death or significant property damage.

(c) When immediate assistance is requested by a deputy or other law enforcement agency.

If a deputy believes an emergency response to any call is appropriate, the deputy shall immediately notify the dispatcher.

309.4 REQUESTING EMERGENCY ASSISTANCE

When requesting emergency assistance, the involved department member should reasonably believe there is an imminent threat to the safety of him/herself or another person, or that assistance is needed to prevent imminent serious harm to the public.

If circumstances permit, the requesting member should provide the following information:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

- Identifying call sign
- Location of the emergency situation
- Suspect information, including weapons
- Reason for the request and type of emergency
- The number of deputies or resources required
- Hazards and any known or potential dangers for responding deputies

In any event where a situation has stabilized and emergency response is not required, the requesting member shall immediately notify the dispatcher.

309.5 SAFETY CONSIDERATIONS

Responding with emergency lights and siren does not relieve the operator of an emergency vehicle of the duty to continue to drive with due regard for the safety of all persons and property, and does not protect the operator from the consequences of reckless disregard for the safety of others. However the deputy may, when responding to a call with an emergency response, and provided there is no endangerment or unnecessary risk to persons and property (Va. Code § 46.2-920):

- Disregard speed limits, while having due regard for safety of persons and property.
- Proceed past any steady or flashing red signal, traffic light, stop sign, or device indicating moving traffic shall stop if the speed of the vehicle is sufficiently reduced to enable it to pass a signal, traffic light, or device with due regard to the safety of persons and property
- Disregard regulations governing a direction of movement of vehiclesturning in specified directions so long as the operator does not endanger life or property.
- Park or stop where it is otherwise prohibited.
- Pass or overtake, with due regard to the safety of persons and property, another vehicle at any intersection.
- Pass or overtake with due regard to the safety of persons and property, while en route to an emergency, stopped or slow-moving vehicles, by going to the left of the stopped or slow-moving vehicle either in a no-passing zone or by crossing the highway centerline.
- Pass or overtake with due regard to the safety of persons and property, while en route to an emergency, stopped or slow-moving vehicles, by going off the paved or main traveled portion of the roadway on the right. Vehicles exempted in this instance will not be required to sound a siren or any device to give automatically intermittent signals.

309.5.1 NUMBER OF DEPUTIES ASSIGNED

The number of deputies assigned to respond to an emergency call or request for assistance should be limited to that which is reasonably necessary.

An emergency response involving more than one sheriff's vehicle should be coordinated by the Dispatch Center to avoid any unanticipated intersecting of response routes. The dispatcher

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

shall notify the Shift Supervisor or field supervisor, who will make a determination regarding the appropriateness of the response and reduce or enhance the response as warranted.

309.6 EMERGENCY EQUIPMENT

Vehicles not equipped with emergency lights and siren are prohibited from initiating or joining in an emergency response. Deputies in such vehicles may provide support to pursuing vehicles as long as the vehicles are operated in compliance with all traffic laws. Those deputies should terminate their involvement in any emergency response immediately upon arrival of a sufficient number of emergency law enforcement vehicles (Va. Code § 46.2-920).

If the emergency equipment on the vehicle should fail to operate, the deputy must terminate the emergency response and continue accordingly. The deputy shall notify the Shift Supervisor, field supervisor or the dispatcher of the equipment failure so that another deputy may be assigned to the emergency response.

309.7 DEPUTY RESPONSIBILITIES

The decision to initiate or continue an emergency response is at the discretion of the deputy. If, in the deputy's judgment, the weather, traffic and road conditions do not permit such a response without unreasonable risk, the deputy may elect to respond to the call without the use of emergency lights and siren at the legal speed limit. In such an event, the deputy should immediately notify the dispatcher. A deputy shall also discontinue an emergency response when directed by a supervisor or as otherwise appropriate.

Upon receiving authorization or determining that an emergency response is appropriate, whenever practicable, a deputy shall immediately give the location from which he/she is responding.

The first deputy arriving at the emergency call should determine whether to increase or reduce the level of the response of additional deputies and shall notify the dispatcher of his/her determination. Any subsequent change in the appropriate response level should be communicated to the dispatcher by the deputy in charge of the scene unless a supervisor assumes this responsibility.

309.8 THE DISPATCH CENTER

When information reasonably indicates that the public is threatened with serious injury or death, or a deputy requests emergency assistance and immediate law enforcement response is needed, the dispatcher shall assign an emergency response and ensure acknowledgement and response of handling and assisting deputies.

309.8.1 RESPONSIBILITIES

Upon notification or assignment of an emergency response, the dispatcher is responsible for:

(a) Confirming the location from which the deputy is responding or requesting assistance.

(b) Attempting to assign the closest available assisting deputies to the location of the emergency call.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) Continuing to obtain and broadcast information as necessary concerning the response and monitoring the situation until it is stabilized or terminated.

(d) Notifying and coordinating allied emergency services (e.g., fire, emergency medical services).

(e) Notifying the Shift Supervisor as soon as practicable.

(f) Controlling all radio communications during the emergency and coordinating assistance under the direction of the Shift Supervisor or field supervisor.

309.9 SUPERVISOR RESPONSIBILITIES

Upon being notified that an emergency response has been initiated or requested, the Shift Supervisor or the field supervisor shall verify that:

(a) The proper response has been initiated.

(b) No more than those deputies reasonably necessary under the circumstances are involved in the response.

(c) Affected outside jurisdictions are being notified as practicable.

The field supervisor shall monitor the response until it has been stabilized or terminated and assert control by directing deputies into or out of the response, if necessary. If, in the supervisor's judgment, the circumstances require additional deputies to be assigned an emergency response, the supervisor may do so.

It is the supervisor's responsibility to terminate an emergency response that, in his/her judgment, is inappropriate due to the circumstances.

When making the decision to authorize an emergency response, the Shift Supervisor or the field supervisor should consider:

- The type of call or crime involved.
- The type and circumstances of the request.
- The necessity of a timely response.
- Weather, traffic and road conditions.
- The location of the responding deputies and the location of the incident.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Canines

310.1 PURPOSE AND SCOPE

This policy establishes guidelines for the use of canines to augment law enforcement services in the community, including but not limited to locating individuals and contraband and apprehending criminal offenders.

310.2 POLICY

It is the policy of the Madison County Sheriff's Office that teams of handlers and canines meet and maintain the appropriate proficiency to effectively and reasonably carry out legitimate law enforcement objectives.

310.3 ASSIGNMENT

Canine teams should be assigned to assist and supplement the Patrol Division to function primarily in assist or cover assignments. However, they may be assigned by the Shift Supervisor to other functions, such as routine calls for service, based on the current operational needs.

Canine teams should generally not be assigned to handle routine matters that will take them out of service for extended periods of time. If such assignment is necessary, it should only be made with the approval of the Shift Supervisor.

310.4 CANINE COORDINATOR

The canine coordinator shall be appointed by and directly responsible to the Patrol Division Supervisor or the authorized designee.

The responsibilities of the coordinator include but are not limited to:

(a) Reviewing all canine use reports to ensure compliance with policy and to identify training issues and other needs of the program.

(b) Maintaining a liaison with the vendor kennel.

(c) Maintaining a liaison with command staff and functional supervisors.

(d) Maintaining a liaison with other agency canine coordinators.

(e) Maintaining accurate records to document canine activities.

(f) Recommending and overseeing the procurement of equipment and services for the teams of handlers and canines.

(g) Ensuring appropriate equipment is identified, documented, and issued to canine teams and maintained appropriately.

(h) Scheduling all canine-related activities.

(i) Ensuring the canine teams are scheduled for regular training to maximize their capabilities.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

310.4.1 REQUIRED EQUIPMENT

The canine coordinator shall develop and maintain a list of equipment required for each canine team.

This list should include but not be limited to:

(a) Collars.

(b) Leashes.

(c) Muzzles.

(d) Food/water bowls.

(e) Grooming supplies.

(f) Exercise/training equipment.

310.5 REQUESTS FOR CANINE TEAMS

Patrol Division members are encouraged to request the use of a canine. Requests for a canine team from department units outside of the Patrol Division shall be reviewed by the Shift Supervisor.

310.5.1 OUTSIDE AGENCY REQUEST

All requests for canine assistance from outside agencies must be approved by the Shift Supervisor and are subject to the following:

(a) Canine teams shall not be used for any assignment that is not consistent with this policy.

(b) The canine handler shall have the authority to decline a request for any specific assignment that he/she deems unsuitable.

(c) Calling out off-duty canine teams is discouraged.

(d) It shall be the responsibility of the canine handler to coordinate operations with agency personnel in order to minimize the risk of unintended injury.

(e) It shall be the responsibility of the canine handler to complete all necessary reports or as directed.

310.5.2 PUBLIC DEMONSTRATION

All public requests for a canine team shall be reviewed and, if appropriate, approved by the canine coordinator prior to making any resource commitment. The canine coordinator is responsible for obtaining resources and coordinating involvement in the demonstration to include proper safety protocols. Canine handlers shall not demonstrate any apprehension work unless authorized to do so by the canine coordinator.

310.6 APPREHENSION GUIDELINES

A canine may be used to locate and apprehend a suspect if the canine handler reasonably believes that the individual has committed, is committing, or is threatening to commit any serious offense and if any of the following conditions exist:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) There is a reasonable belief the suspect poses an imminent threat of violence or serious harm to the public, any deputy, or the handler.

(b) The suspect is physically resisting or threatening to resist arrest and the use of a canine reasonably appears to be necessary to overcome such resistance.

(c) The suspect is believed to be concealed in an area where entry by other than the canine would pose a threat to the safety of deputies or the public.

It is recognized that situations may arise that do not fall within the provisions set forth in this policy. Such events require consideration of the totality of the circumstances and the use of an objective reasonableness standard applied to the decision to use a canine.

Absent a reasonable belief that a suspect has committed, is committing, or is threatening to commit a serious offense, mere flight from a pursuing deputy, without any of the above conditions, shall not serve as the basis for the use of a canine to apprehend a suspect.

Use of a canine to locate and apprehend a suspect wanted for a lesser criminal offense than those identified above requires approval from the Shift Supervisor. Absent a change in circumstances that presents an imminent threat to deputies, the canine, or the public, such canine use should be conducted on-leash or under conditions that minimize the likelihood the canine will bite or otherwise injure the individual.

In all applications, once the suspect has been located and no longer reasonably appears to present a threat or risk of escape, the handler should secure the canine as soon as it becomes reasonably practicable.

If the canine has apprehended the suspect with a secure bite, and the handler believes that the suspect no longer poses a threat, the handler should promptly command the canine to release the suspect.

310.6.1 PREPARATION FOR DEPLOYMENT

Prior to the use of a canine to search for or apprehend any suspect, the canine handler and/or the supervisor on-scene should carefully consider all pertinent information reasonably available at the time. The information should include but is not limited to:

(a) The nature and seriousness of the suspected offense.

(b) Whether violence or weapons were used or are anticipated.

(c) The degree of resistance or threatened resistance, if any, the suspect has shown.

(d) The suspect’s known or perceived age.

(e) The potential for injury to deputies or the public caused by the suspect if the canine is not utilized.

(f) Any potential danger to the public and/or other deputies at the scene if the canine is released.

(g) The potential for the suspect to escape or flee if the canine is not utilized.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

As circumstances permit, the canine handler should make every reasonable effort to communicate and coordinate with other involved members to minimize the risk of unintended injury.

It is the canine handler's responsibility to evaluate each situation and determine whether the use of a canine is appropriate and reasonable. The canine handler shall have the authority to decline the use of the canine whenever he/she deems deployment is unsuitable.

A supervisor who is sufficiently apprised of the situation may prohibit deploying the canine.

Unless otherwise directed by a supervisor, assisting members should take direction from the handler in order to minimize interference with the canine.

310.6.2 WARNINGS AND ANNOUNCEMENTS

Unless it would increase the risk of injury or escape, a clearly audible warning announcing that a canine will be used if the suspect does not surrender should be made prior to releasing a canine. The handler should allow a reasonable time for a suspect to surrender and should quiet the canine momentarily to listen for any verbal response to the warning. If feasible, other members should be in a location opposite the warning to verify that the announcement could be heard. If available, warnings given in other languages should be used as necessary.

If a warning is not to be given, the canine handler, when practicable, should first advise the supervisor of his/her decision before releasing the canine. In the event of an apprehension, the handler shall document in any related report how the warning was given and, if none was given, the reasons why.

310.6.3 REPORTING DEPLOYMENTS, BITES, AND INJURIES

Handlers should document canine deployments in a canine use report. Whenever a canine deployment results in a bite or causes injury to an intended suspect, a supervisor should be promptly notified and the injuries documented in a canine use report. The injured person shall be promptly treated by Emergency Medical Services personnel and, if appropriate, transported to an appropriate medical facility for further treatment. The deployment and injuries should also be included in any related incident or arrest report.

Any unintended bite or injury caused by a canine, whether on- or off-duty, shall be promptly reported to the canine coordinator. Unintended bites or injuries caused by a canine should be documented in an administrative report, not in a canine use report.

If an individual alleges an injury, either visible or not visible, a supervisor shall be notified and both the individual's injured and uninjured areas shall be photographed as soon as practicable after first tending to the immediate needs of the injured party. Photographs shall be retained as evidence in accordance with current department evidence procedures. The photographs shall be retained until the criminal proceeding is completed and the time for any related civil proceeding has expired.

310.7 NON-APPREHENSION GUIDELINES

Properly trained canines may be used to track or search for non-criminals (e.g., lost children, individuals who may be disoriented or in need of medical attention). The canine handler is

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

responsible for determining the canine's suitability for such assignments based on the conditions and the particular abilities of the canine. When the canine is deployed in a search or other non-apprehension operation, the following guidelines apply:

(a) Absent a change in circumstances that presents an imminent threat to deputies, the canine, or the public, such applications should be conducted on-leash or under conditions that minimize the likelihood the canine will bite or otherwise injure the individual, if located.

(b) Unless otherwise directed by a supervisor, assisting members should take direction from the handler in order to minimize interference with the canine.

(c) Throughout the deployment, the handler should periodically give verbal assurances that the canine will not bite or hurt the individual and encourage the individual to make him/herself known.

(d) Once the individual has been located, the handler should place the canine in a down-stay or otherwise secure it as soon as reasonably practicable.

310.7.1 ARTICLE DETECTION

A canine trained to find objects or property related to a person or crime may be used to locate or identify articles. A canine search should be conducted in a manner that minimizes the likelihood of unintended bites or injuries.

310.7.2 NARCOTICS DETECTION

A canine trained in narcotics detection may be used in accordance with current law and under certain circumstances, including:

(a) The search of vehicles, buildings, bags, and other articles.

(b) Assisting in the search for narcotics during a search warrant service.

(c) Obtaining a search warrant by using the narcotics-detection trained canine in support of probable cause.

A narcotics-detection trained canine will not be used to search a person for narcotics unless the canine is trained to passively indicate the presence of narcotics.

310.7.3 BOMB/EXPLOSIVE DETECTION

Because of the high risk of danger to the public and deputies when a bomb or other explosive device is suspected, the use of a canine team trained in explosive detection may be considered. When available, an explosive-detection canine team may be used in accordance with current law and under certain circumstances, including:

(a) Assisting in the search of a building, structure, area, vehicle, or article where an actual or suspected explosive device has been reported or located.

(b) Assisting with searches at transportation facilities and vehicles (e.g., buses, airplanes, trains).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) Preventive searches at special events, VIP visits, official buildings, and other restricted areas. Searches of individuals should remain minimally intrusive and shall be strictly limited to the purpose of detecting explosives.

(d) Assisting in the search of scenes where an explosion has occurred and an explosive device or secondary explosive device is suspected.

At no time will an explosive-detection trained canine be used to render a suspected device safe or clear.

310.8 HANDLER SELECTION

The minimum qualifications for the assignment of canine handler include:

(a) A deputy who is currently off probation.

(b) Residing in an adequately fenced single-family residence (minimum 5-foot-high fence with locking gates).

(c) A garage that can be secured and can accommodate a canine vehicle.

(d) Living within 30 minutes travel time from the Madison County, Virginia County limits.

(e) Agreeing to be assigned to the position for a minimum of three years.

310.9 HANDLER RESPONSIBILITIES

The canine handler shall ultimately be responsible for the health and welfare of the canine and shall ensure that the canine receives proper nutrition, grooming, training, medical care, affection, and living conditions.

The canine handler will be responsible for the following:

(a) Except as required during appropriate deployment, the handler shall not expose the canine to any foreseeable and unreasonable risk of harm.

(b) The handler shall maintain all department equipment under his/her control in a clean and serviceable condition.

(c) When not in service, the handler shall maintain the canine vehicle in a locked garage, away from public view.

(d) When a handler is off-duty for an extended number of days, the assigned canine vehicle should be stored at the Madison County Sheriff's Office facility.

(e) Handlers shall permit the canine coordinator to conduct spontaneous on-site inspections of affected areas of their homes as well as their canine vehicles to verify that conditions and equipment conform to this policy.

(f) Any changes in the living status of the handler that may affect the lodging or environment of the canine shall be reported to the canine coordinator as soon as possible.

(g) When off-duty, the canine shall be in a kennel provided by the County at the home of the handler. When a canine is kenneled at the handler’s home, the gate shall be secured with a lock. When off-duty, the canine may be let out of the kennel while under the direct control of the handler.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(h) The canine should be permitted to socialize in the home with the handler's family for short periods of time and under the direct supervision of the handler.

(i) Under no circumstances will the canine be lodged at another location unless approved by the canine coordinator or Shift Supervisor.

(j) When off-duty, the handler shall not involve the canine in any law enforcement activity or official conduct unless approved in advance by the canine coordinator or Shift Supervisor.

(k) Whenever a canine handler is off-duty for an extended number of days, it may be necessary to temporarily relocate the canine. In those situations, the handler shall give reasonable notice to the canine coordinator so that appropriate arrangements can be made.

310.9.1 CANINE IN PUBLIC AREAS

The canine should be kept on a leash when in areas that allow access to the public. Exceptions to this rule would include specific law enforcement operations for which the canine is trained.

(a) A canine shall not be left unattended in any area to which the public may have access.

(b) When the canine vehicle is left unattended, all windows and doors shall be secured in such a manner as to prevent unauthorized access to the canine. The handler shall also ensure that the unattended vehicle remains inhabitable for the canine.

310.10 HANDLER COMPENSATION

The canine handler shall be available for call-out under conditions specified by the canine coordinator.

The canine handler shall be compensated for time spent in the care, feeding, grooming and other needs of the canine in accordance with the Fair Labor Standards Act (FLSA), and according to the terms of the agreement between the handler and the County (29 USC § 207).

310.11 CANINE INJURY AND MEDICAL CARE

In the event that a canine is injured, or there is an indication that the canine is not in good physical condition, the injury or condition will be reported to the canine coordinator or Shift Supervisor as soon as practicable and appropriately documented.

All medical attention shall be rendered by the designated canine veterinarian, except during an emergency where treatment should be obtained from the nearest available veterinarian. All records of medical treatment shall be maintained in the handler's personnel file.

310.12 TRAINING

Before assignment in the field, each canine team shall be trained and certified to meet current nationally recognized standards or other recognized and approved certification standards. Cross-trained canine teams or those canine teams trained exclusively for the detection of narcotics and/or explosives also shall be trained and certified to meet current nationally recognized standards or other recognized and approved certification standards established for their particular skills.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Canines

The canine coordinator shall be responsible for scheduling periodic training for all department members in order to familiarize them with how to conduct themselves in the presence of department canines. Because canines may be exposed to dangerous substances such as opioids, as resources are available, the canine coordinator should also schedule periodic training for the canine handlers about the risks of exposure and treatment for it.

All canine training shall be conducted while on-duty unless otherwise approved by the canine coordinator or Shift Supervisor.

310.12.1 CONTINUED TRAINING

Each canine team shall thereafter be recertified to a current nationally recognized standard or other recognized and approved certification standards on an annual basis. Additional training considerations are as follows:

(a) Canine teams should receive training as defined in the current contract with the Madison County Sheriff's Office canine training provider.

(b) Canine handlers are encouraged to engage in additional training with approval of the canine coordinator.

(c) To ensure that all training is consistent, no handler, trainer or outside vendor is authorized to train to a standard that is not reviewed and approved by the Department.

310.12.2 FAILURE TO SUCCESSFULLY COMPLETE TRAINING

Any canine team failing to graduate or obtain certification shall not be deployed in the field for tasks the team is not certified to perform until graduation or certification is achieved. When reasonably practicable, pending successful certification, the canine handler shall be temporarily reassigned to regular patrol duties.

310.12.3 TRAINING RECORDS

All canine training records shall be maintained in the canine handler’s and the canine’s training file.

310.12.4 TRAINING AIDS

Training aids are required to effectively train and maintain the skills of canines. Deputies possessing, using, or transporting controlled substances or explosives for canine training purposes must comply with federal and state requirements. Alternatively, the Madison County Sheriff's Office may work with outside trainers with the applicable licenses or permits.

310.12.5 CONTROLLED SUBSTANCE TRAINING AIDS

Deputies acting in the performance of their official duties may possess or transfer controlled substances for the purpose of narcotics-detection canine training in compliance with state and federal laws and in compliance with applicable state requirements (21 USC § 823(f); Va. Code § 18.2-250).

The Sheriff or the authorized designee may authorize a member to seek a court order to allow controlled substances seized by the Madison County Sheriff's Office to be possessed by

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

the member or a narcotics-detection canine trainer who is working under the direction of this department for training purposes, provided the controlled substances are no longer needed as criminal evidence (Va. Code § 19.2-386.23).

As an alternative, the Sheriff or the authorized designee may request narcotics training aids from the Drug Enforcement Administration (DEA).

These procedures are not required if the canine handler uses commercially available synthetic substances that are not controlled narcotics.

310.12.6 CONTROLLED SUBSTANCE PROCEDURES

Due to the responsibilities and liabilities involved with possessing readily usable amounts of controlled substances and the ever-present danger of the canine's accidental ingestion of these controlled substances, the following procedures shall be strictly followed:

(a) All controlled substance training samples shall be weighed and tested prior to dispensing to the individual canine handler or trainer.

(b) The weight and test results shall be recorded and maintained by this department.

(c) Any person possessing controlled substance training samples pursuant to court order or DEA registration shall maintain custody and control of the controlled substances and shall keep records regarding any loss of, or damage to, those controlled substances.

(d) All controlled substance training samples will be inspected, weighed, and tested quarterly. The results of the quarterly testing shall be recorded and maintained by the canine coordinator with a copy forwarded to the dispensing agency.

(e) All controlled substance training samples will be stored in locked, airtight, and watertight cases at all times, except during training. The locked cases shall be secured in the trunk of the canine handler's assigned patrol vehicle during transport and stored in an appropriate locked container. There are no exceptions to this procedure.

(f) The canine coordinator shall periodically inspect every controlled substance training sample for damage or tampering and take any appropriate action.

(g) Any unusable controlled substance training samples shall be returned to the Property and Evidence Section or to the dispensing agency.

(h) All controlled substance training samples shall be returned to the dispensing agency upon the conclusion of the training or upon demand by the dispensing agency.

(i) An annual, unannounced inventory of controlled substances used for canine training shall be conducted and documented as directed by the Sheriff or the authorized designee.

310.12.7 EXPLOSIVE TRAINING AIDS

Deputies may possess, transport, store, or use explosives or destructive devices in compliance with state and federal laws (18 USC § 842; 27 CFR 555.41; Va. Code § 18.2-85).

Explosive training aids designed specifically for canine teams should be used whenever feasible. Due to the safety concerns in the handling and transportation of explosives, inert or non-hazardous

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

training aids should be employed whenever feasible. The use of explosives or destructive devices for training aids by canine teams is subject to the following:

(a) All explosive training aids, when not in use, shall be properly stored in a secure facility appropriate for the type of materials.

(b) An inventory ledger shall be maintained to document the type and quantity of explosive training aids that are stored.

(c) The canine coordinator shall be responsible for verifying the explosive training aids on hand against the inventory ledger once each quarter.

(d) Only members of the canine team shall have access to the explosive training aids storage facility.

(e) A primary and secondary custodian will be designated to minimize the possibility of loss of explosive training aids during and after the training. Generally, the handler will be designated as the primary custodian while the trainer or authorized second person on-scene will be designated as the secondary custodian.

(f) Any lost or damaged explosive training aids shall be promptly reported to the canine coordinator, who will determine if any further action will be necessary. Any loss of explosives will be reported to the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Domestic or Family Violence

311.1 PURPOSE AND SCOPE

The purpose of this policy is to provide the guidelines necessary to deter, prevent and reduce domestic or family violence through vigorous enforcement and to address domestic or family violence as serious crimes against society. The policy specifically addresses legal mandates and the commitment of the Madison County Sheriff's Office to take enforcement action when appropriate, to provide assistance to victims and to guide deputies in the investigation of domestic or family violence (Va. Code § 9.1-1300).

311.1.1 DEFINITIONS

Definitions related to this policy include:

Court order - All forms of orders related to domestic or family violence, that have been issued by a court of this state or another, whether civil or criminal, regardless of whether service has been made.

Domestic violence - A pattern of physically, sexually, and/or emotionally abusive behaviors used by one person to assert power or maintain control over another in the context of an intimate partner or family relationship. For the purposes of this policy, the term includes family abuse, which is any act involving violence, force, or threat that results in bodily injury or that places another person in reasonable fear of death, sexual assault, or bodily injury, and that is committed by a person against (Va. Code § 16.1-228):

(a) The person's spouse or former spouse, regardless of whether the person resides in the same home.

(b) The person's parents, stepparents, grandparents, grandchildren, children, stepchildren, sibling, or half-sibling regardless of whether the person reside in the same home.

(c) The person's relative by marriage (i.e., in-laws), if residing in the same home.

(d) A person with whom the person has a child in common, whether or not they have been married or resided together at any time.

(e) Another person or child with whom the person lives or has lived within the previous 12 months.

311.2 POLICY

The Madison County Sheriff's Office’s response to incidents of domestic or family violence and violations of related court orders shall stress enforcement of the law to protect the victim and shall communicate the philosophy that domestic or family violence is criminal behavior. It is also the policy of this department to facilitate victims’ and offenders’ access to appropriate civil remedies and community resources whenever feasible.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

311.3 OFFICER SAFETY

The investigation of domestic or family violence cases often places deputies in emotionally charged and sometimes highly dangerous environments. No provision of this policy is intended to supersede the responsibility of all deputies to exercise due caution and reasonable care in providing for the safety of any deputies and parties involved.

311.4 INVESTIGATIONS

The following guidelines should be followed by deputies when investigating domestic or family violence cases:

(a) Calls of reported, threatened, imminent, or ongoing domestic or family violence and the violation of any court order are of extreme importance and should be considered among the highest response priorities. This includes incomplete 9-1-1 calls.

(b) When practicable, deputies should obtain and document statements from the victim, the suspect, and any witnesses, including children, in or around the household or location of occurrence.

(c) Deputies should list the full name and date of birth (and school if available) of each child who was present in the household at the time of the offense. The names of other children who may not have been in the house at that particular time should also be obtained for follow-up.

(d) When practicable and legally permitted, video or audio record all significant statements and observations.

(e) All injuries should be photographed, regardless of severity, taking care to preserve the victim's personal privacy. Where practicable, photographs should be taken by a person of the same sex. Victims whose injuries are not visible at the time of the incident should be asked to contact the Investigation Division in the event that the injuries later become visible.

(f) Deputies should request that the victim complete and sign an authorization for release of medical records related to the incident when applicable.

(g) If the suspect is no longer at the scene, deputies should make reasonable efforts to locate the suspect to further the investigation, provide the suspect with an opportunity to make a statement, and make an arrest or seek an arrest warrant if appropriate.

(h) Seize any firearms or other dangerous weapons in the home, if appropriate and legally permitted, for safekeeping or as evidence.

(i) When completing an incident or arrest report for violation of a court order, deputies should include specific information that establishes that the offender has been served, including the date the offender was served, the name of the agency that served the order, and the provision of the order that the subject is alleged to have violated. When reasonably available, the arresting deputy should attach a copy of the order to the incident or arrest report.

(j) Deputies should take appropriate enforcement action when there is probable cause to believe an offense has occurred. Factors that should not be used as sole justification for declining to take enforcement action include:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1. Whether the suspect lives on the premises with the victim.
2. Claims by the suspect that the victim provoked or perpetuated the violence.
3. The potential financial or child custody consequences of arrest.
4. The physical or emotional state of either party.
5. Use of drugs or alcohol by either party.
6. Denial that the violence occurred where evidence indicates otherwise.
7. A request by the victim not to arrest the suspect.
8. Location of the incident (public/private).
9. Speculation that the complainant may not follow through with the prosecution.
10. Actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, disability, or marital status, of the victim or suspect.
11. The social status, community status, or professional position of the victim or suspect.

(k) If the incident involves a law enforcement officer as the alleged suspect or predominant physical aggressor, deputies should notify the on-duty supervisor, Captain and the Sheriff (Va. Code § 9.1-1300).

1. If the involved law enforcement officer is a member of an outside agency, the on-duty supervisor should notify the respective agency.
2. If the involved law enforcement officer is a member of this department, the on-duty supervisor should notify the Sheriff to expedite presentment of the case to the Commonwealth's attorney.

311.4.1 IF A SUSPECT IS ARRESTED

If a suspect is arrested, deputies should:

(a) Advise the victim that there is no guarantee the suspect will remain in custody.

(b) Provide the victim’s contact information to the jail staff to enable notification of the victim upon the suspect’s release from jail.

(c) Advise the victim whether any type of court order will be in effect when the suspect is released from jail.

311.4.2 IF NO ARREST IS MADE

If no arrest is made, the deputy should:

(a) Advise the parties of any options, including, but not limited to:

1. Voluntary separation of the parties.
2. Appropriate resource referrals (e.g., counselors, friends, relatives, shelter homes, victim witness assistance).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Document the resolution in a report.

311.5 VICTIM ASSISTANCE

Because victims may be traumatized or confused, deputies should be aware that a victim's behavior and actions may be affected.

(a) Victims shall be provided with the department domestic or family violence information handout, even if the incident may not rise to the level of a crime (Va. Code § 19.2-81.3; Va. Code § 19.2-11.01).

(b) Victims shall also be alerted to any available victim advocates, shelters, legal assistance agencies, and community resources.

(c) When an involved person requests law enforcement assistance while removing essential items of personal property, deputies should stand by for a reasonable amount of time.

(d) If the victim has sustained injury or complains of pain, deputies shall seek medical assistance for the victim as soon as practicable.

(e) Deputies should ask the victim whether the victim has a safe place to stay and assist in arranging transportation to an alternate shelter if the victim expresses a concern for their safety or if the deputy determines that a need exists (Va. Code § 19.2-81.3).

(f) Deputies should make reasonable efforts to ensure that any children or dependent adults who are under the supervision of the suspect or victim are being properly cared for.

(g) If appropriate, deputies shall seek or assist the victim in obtaining an emergency order (Va. Code § 19.2-152.8).

(h) When a victim makes the request, a deputy shall transport or arrange for the transportation of the person to a hospital or to appear before a magistrate (Va. Code § 19.2-81.3).

See attachment: 311 VA Summary of Crime Victim and Witness Rights Act.pdf

311.6 DISPATCH ASSISTANCE

All calls of domestic or family violence, including incomplete 9-1-1 calls, should be dispatched as soon as practicable.

Dispatchers are not required to verify the validity of a court order before dispatching a deputy to a request for assistance. The existence or validity of any applicable court order should be determined and promptly made available to the assigned deputy once dispatched. Deputies should request that dispatchers check whether any of the involved persons are subject to the terms of a court order.

311.7 FOREIGN COURT ORDERS

Various types of orders may be issued in domestic or family violence cases. Any foreign court order properly issued by a court of another state, Indian tribe or territory shall be enforced by deputies as if it were the order of a court in this state. An order should be considered properly

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

issued when it reasonably appears that the issuing court has jurisdiction over the parties and reasonable notice and opportunity to respond was given to the party against whom the order was issued (18 USC § 2265). An otherwise valid out-of-state court order shall be enforced, regardless of whether the order has been properly registered with this state (Va. Code § 16.1-279.1).

A deputy may rely upon a copy of a foreign order or other suitable evidence which has been provided to him/her by any source and may also rely upon the statement of any person protected by the order that the order remains in effect (Va. Code § 16.1-279.1).

311.8 VERIFICATION OF COURT ORDERS

Determining the validity of a court order, particularly an order from another jurisdiction, can be challenging. Therefore, in determining whether there is probable cause to make an arrest for a violation of any court order, deputies should carefully review the actual order when available and, where appropriate and practicable:

(a) Ask the subject of the order about his/her notice or receipt of the order, knowledge of its terms and efforts to respond to the order.

(b) Check available records or databases that may show the status or conditions of the order.

(c) Contact the issuing court to verify the validity of the order.

(d) Contact a law enforcement official from the jurisdiction where the order was issued to verify information.

Deputies should document in an appropriate report their efforts to verify the validity of an order, regardless of whether an arrest is made. Deputies should contact a supervisor for clarification when needed.

311.9 STANDARDS FOR ARRESTS

Deputies investigating reported domestic or family violence (Va. Code § 19.2-81.3):

(a) Shall arrest the predominant aggressor when there is probable cause to believe that the person:

1. Committed an offense of assault and battery against a family or household member (Va. Code § 18.2-57.2).
2. Violated a protective order pursuant to Va. Code § 16.1-253.2.
3. Violated a protective order pursuant to Va. Code § 18.2-60.4 by committing an act of physical aggression.
    - However, an arrest need not be made if a supervisor has approved a course of action other than arrest.

(b) Shall consider the following when determining whether a person is a predominant physical aggressor:

1. The identity of the first aggressor

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. The protection of the health and safety of family and household members
3. Prior complaints of domestic or family violence by the suspect involving family or household members
4. In incidents involving a violation of a protective order, any prior acts of violence, force, or threat (as defined by Va. Code § 19.2-152.7:1) against the protected person or the protected person's family or household members
5. The severity of the injuries inflicted on persons involved in the incident
6. Whether any injuries were inflicted in self-defense
7. Witness statements
8. Any other observations

(c) Should make an arrest in any other incident involving domestic or family violence when there is probable cause to believe that an offense of assault and battery against a family member or a violation of a protective order has occurred, regardless of whether the offense was committed within the presence of the deputy. Any decision not to arrest shall be approved by a supervisor.

(d) Should make an arrest if circumstances indicate that the person has been previously accused of domestic or family violence.

1. Information about calls for family abuse, domestic violence, and/or stalking entered into department records should be used to improve handling of these types of calls and track repeat offenders.

311.9.1 REQUESTS FOR EMERGENCY PROTECTIVE ORDERS

When a deputy makes an arrest for an offense of assault and battery committed against a family or household member, the deputy shall petition the court for an emergency protective order at the time that the suspect is brought before the magistrate. A request for an emergency protective order is not required if the person arrested is a minor (Va. Code § 19.2-81.3).

Regardless of whether an arrest is made, a deputy may petition the court for an emergency protective order in any other circumstances where the deputy has probable cause to believe that a danger of domestic or family violence exists.

311.10 REPORTS AND RECORDS

When investigating an incident of domestic or family violence, whether or not an arrest is made, a deputy shall complete a written report. The report shall include the following (Va. Code § 19.2-81.3):

(a) Whether any arrests were made, if so, the number of arrests made.

(b) The probable cause to believe that an incident of domestic or family violence has occurred.

(c) The location where the incident of domestic or family violence occurred.

(d) The special circumstances that dictated a course of action other than arrest.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Upon request, deputies shall make a summary of the report available to the victim or persons protected by an order.

311.11 SERVICE OF COURT ORDERS

Upon receipt of an order from the issuing court, deputies serving the order shall (Va. Code § 19.2-152.8; Va. Code § 19.2-152.9; Va. Code § 19.2-152.10; Va. Code § 16.1-279.1; Va. Code § 19.2-387.1):

(a) Verify the identifying information and make modification as necessary in the Virginia Criminal Information Network (VCIN).

(b) Serve the respondent with the order.

(c) Enter the date and time of service and other appropriate information into VCIN.

(d) File any required proof of service forms with the issuing court.

311.12 ORDERS REQUIRED TO BE ENTERED INTO VCIN

The Records Manager shall ensure protective orders are entered into VCIN (Va. Code § 19.2-152.8; Va. Code § 19.2-152.9; Va. Code § 19.2-152.10; Va. Code § 16.1-279.1; Va. Code § 19.2-387.1).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Search and Seizure

312.1 PURPOSE AND SCOPE

Both the federal and state constitutions provide every individual with the right to be free from unreasonable searches and seizures. This policy provides general guidelines for Madison County Sheriff's Office personnel to consider when dealing with search and seizure issues.

312.2 POLICY

It is the policy of the Madison County Sheriff's Office to respect the fundamental privacy rights of individuals. Members of this department will conduct searches in strict observance of the constitutional rights of persons being searched. All seizures by this department will comply with relevant federal and state law governing the seizure of persons and property.

The Department will provide relevant and current training to deputies as guidance for the application of current law, local community standards and prosecutorial considerations regarding specific search and seizure situations, as appropriate.

312.3 SEARCHES

The U.S. Constitution generally provides that a valid warrant is required in order for a search to be valid. There are, however, several exceptions to the rule that permit a warrantless search.

Examples of law enforcement activities that are exceptions to the general warrant requirement include, but are not limited to, searches pursuant to:

- Valid consent.
- Incident to a lawful arrest.
- Legitimate community caretaking interests.
- Vehicle searches under certain circumstances.
- Exigent circumstances.

Certain other activities are recognized by federal and state courts and by certain statutes as legitimate law enforcement activities that also do not require a warrant. Such activities may include seizure and examination of abandoned property and observations of activities and property located on open public areas.

Because case law regarding search and seizure is constantly changing and subject to interpretation by the courts, each member of this department is expected to act in each situation according to current training and his/her familiarity with clearly established rights as determined by case law.

Whenever practicable, deputies are encouraged to contact a supervisor to resolve questions regarding search and seizure issues prior to electing a course of action.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

312.4 SEARCH PROTOCOL

Although conditions will vary, and officer safety and other exigencies must be considered in every search situation, the following guidelines should be followed whenever circumstances permit:

(a) Members of this department will strive to conduct searches with dignity and courtesy.

(b) Deputies should explain to the person being searched the reason for the search and how the search will be conducted.

(c) Searches should be carried out with due regard and respect for private property interests and in a manner that minimizes damage. Property should be left in a condition as close as reasonably possible to its pre-search condition.

(d) In order to minimize the need for forcible entry, an attempt should be made to obtain keys, combinations or access codes when a search of locked property is anticipated.

(e) Whenever practicable, a search should not be conducted by a lone deputy. A cover deputy should be positioned to ensure safety and should not be involved in the search.

(f) When the person to be searched is of the opposite sex as the searching deputy, a reasonable effort should be made to summon a deputy of the same sex as the subject to conduct the search. When it is not practicable to summon a deputy of the same sex as the subject, the following guidelines should be followed:

1. Another deputy or a supervisor should witness the search.
2. The deputy should not search areas of the body covered by tight-fitting clothing, sheer clothing or clothing that could not reasonably conceal a weapon.

312.5 DOCUMENTATION

Deputies are responsible for documenting any search and ensuring that any required reports are sufficient including, at minimum, documentation of:

- Reason for the search.
- Any efforts used to minimize the intrusiveness of any search (e.g., asking for consent or keys).
- What, if any, injuries or damage occurred.
- All steps taken to secure property.
- The results of the search including a description of any property or contraband seized.
- If the person searched is the opposite sex, any efforts to summon a deputy of the same sex as the person being searched and the identification of any witness deputy.

Supervisors shall review reports to ensure the reports are accurate, that actions are properly documented and that current legal requirements and department policy have been met.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Child Abuse

313.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the investigation of suspected child abuse. This policy also addresses when Madison County Sheriff's Office members are required to notify Virginia Department of Social Service (VDSS) or their local department of social services' Child Protective Services (CPS) of suspected child abuse.

313.1.1 DEFINITIONS

Definitions related to this policy include:

Child - Unless otherwise specified by a cited statute, a child is any person under the age of 18 years.

Child abuse - Any offense or attempted offense involving violence or neglect with a child victim when committed by a person responsible for the child’s care or any other act that would mandate notification to a social service agency.

313.2 POLICY

The Madison County Sheriff's Office will investigate all reported incidents of alleged criminal child abuse and ensure CPS is notified as required by law.

313.3 MANDATORY NOTIFICATION

Members of the Madison County Sheriff's Office shall notify CPS when the member has reason to suspect that a child may be a victim of abuse or neglect (Va. Code § 63.2-1509).

For purposes of notification, abuse and neglect include but are not limited to the following (Va. Code § 63.2-100; 22 VAC 40-705-30):

(a) An intentional act or omission by the caretaker of a child that causes, threatens, or permits a physical or mental injury to the child

(b) The creation by the caretaker of a child of a substantial risk of death, disfigurement, or impairment of bodily or mental functions

(c) The failure by the caretaker of a child to provide adequate food, clothing, shelter, supervision, or medical care

(d) The commission, or the allowance by the caretaker of a child or that caretaker's intimate partner, of any sexual exploitation of or sexual act upon the child

(e) The commission by any person of sex trafficking or other severe forms of trafficking against a child

313.3.1 NOTIFICATION PROCEDURE

Notification should occur immediately, but no later than 24 hours after becoming aware of the abuse or neglect, by directly contacting the local CPS office or by calling the child abuse and neglect hotline. The report should include the following information, if known (Va. Code § 63.2-1509):

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) The name, address and telephone number of both the child and parent or other person responsible for the child's care.

(b) The child's date of birth, age, sex and race.

(c) The names and ages of the other persons who reside with the child and their relationship to the child.

(d) Whether or not there is a family member who can protect the child.

(e) The name, address and telephone number of the suspected abuser and his/her relationship to the child.

(f) The nature and extent of the abuse or neglect, including any knowledge of prior maltreatment of the child or his/her siblings.

(g) Any special language needs of the family.

(h) Any child or adult developmental issues.

(i) Whether the child has a disability and the ways in which the disability affects the child's functioning and care.

(j) The name and contact information for the investigating member.

(k) Any other pertinent information.

313.4 QUALIFIED INVESTIGATORS

Qualified investigators should be available for child abuse investigations. These investigators should:

(a) Conduct interviews in child-appropriate interview facilities.

(b) Be familiar with forensic interview techniques specific to child abuse investigations.

(c) Present all cases of alleged child abuse to the prosecutor for review.

(d) Coordinate with other enforcement agencies, social service agencies and school administrators as needed.

(e) Provide referrals to therapy services, victim advocates, guardians and support for the child and family as appropriate.

(f) Participate in or coordinate with multidisciplinary investigative teams as applicable.

313.5 INVESTIGATIONS AND REPORTING

In all reported or suspected cases of child abuse, deputies shall write a report even if the allegations appear unfounded or unsubstantiated.

In accordance with the Investigation Protocol of the Madison County Child Abuse Multi-Disciplinary Team (MDT) Memorandum of Agreement, Investigations and reports related to suspected cases of child abuse should address, as applicable:

(a) The overall basis for the contact. This should be done by the investigating deputy in all circumstances where a suspected child abuse victim was contacted.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) The exigent circumstances that existed if deputies interviewed the child victim without the presence of a parent or guardian.

(c) Any relevant statements the child may have made and to whom he/she made the statements.

(d) If a child was taken into protective custody, the reasons, the name and title of the person making the decision, and why other alternatives were not appropriate.

(e) Documentation of any visible injuries or any injuries identified by the child. This should include photographs of such injuries, if practicable.

(f) Whether the child victim was transported for medical treatment or a medical examination.

(g) Whether the victim identified a household member as the alleged perpetrator, and a list of the names of any other children who may reside in the residence.

(h) Identification of any prior related reports or allegations of child abuse, including other jurisdictions, as reasonably known.

(i) Previous addresses of the victim and suspect.

(j) Other potential witnesses who have not yet been interviewed, such as relatives or others close to the victim's environment.

All cases of an unexplained death of a child should be investigated as thoroughly as if it had been a case of suspected child abuse (e.g., a sudden or unexplained death of an infant).

See attachment: VA Madison County Child Abuse Multi-Disciplinary Team (MDT Agreement July 1 2020.pdf

313.6 PROTECTIVE CUSTODY

Before taking any child into protective custody, the deputy should make reasonable attempts to contact CPS. Generally, removal of a child from his/her family, guardian or other responsible adult should be left to the child welfare authorities when they are present or have become involved in an investigation.

Generally, members of this department should remove a child from his/her parent or guardian without a court order only when no other effective alternative is reasonably available and immediate action reasonably appears necessary to protect the child. Prior to taking a child into protective custody, the deputy should take reasonable steps to deliver the child to another qualified parent or legal guardian unless it reasonably appears that the release would endanger the child or result in abduction. If this is not a reasonable option, the deputy shall ensure that the child is delivered to CPS.

Whenever practicable, the deputy should inform a supervisor of the circumstances prior to taking a child into protective custody. If prior notification is not practicable, deputies should contact a supervisor promptly after taking a child into protective custody.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Children may only be removed from a parent or guardian pursuant to a court order. However, children may be removed for up to 72 hours without a court order or consent from a parent or guardian when (Va. Code § 63.2-1517):

(a) It appears that there is an imminent danger to the child's life or health.

(b) A court order is not immediately obtainable.

(c) The court has set up procedures for placing such children.

(d) The parent or guardian is notified as soon as practicable following the removal.

(e) A report is made to the CPS.

(f) The court is notified as soon as possible and a petition for an emergency removal order is filed before the expiration of the 72-hour period.

313.6.1 SAFE HAVEN LAW

A person may safely deliver a child who is 30 days old or younger to a hospital that provides 24-hour emergency services or to an attended emergency medical service agency that employs emergency medical services personnel (Va. Code § 8.01-226.5:2; Va. Code § 16.1-228; Va. Code § 18.2-371; Va. Code § 18.2-371.1; Va. Code § 40.1-103; Va. Code § 63.2-100).

313.7 INTERVIEWS

In accordance with the attached Off-Site Forensic Interview Protocol, the Foothills Child Advocacy Center will will accept children for courtesy forensic interviews that are referred by DSS Child Protective Services ("CPS") or the Sheriff's Office and are alleged victims in CPS and/or Sheriff's Office investigations and who are under age 18 at the time of the interview and who are alleged victims of criminal sexual assault or physical abuse.

The assigned CPS and Sheriff's Office investigator will first make contact with each other to decide on a time when both team members can be present at the interview. The CPS or Sheriff's Office investigator will make contact with the parent or guardian of the child to decide on a time that the parent/guardian or other designated person can bring the child to the appointment. Interviews will be scheduled in accordance with the guidance set forth in the Off-Site Forensic Interview Protocol.

See attachment: VA Madison County SO - Off Site Forensic Interview Protocol (2017).pdf

313.7.1 PRELIMINARY INTERVIEWS

Absent extenuating circumstances or impracticality, deputies should record the preliminary interview with suspected child abuse victims. Deputies should avoid multiple interviews with a child victim and should attempt to gather only the information necessary to begin an investigation. When practicable, investigating deputies should defer interviews until a person who is specially trained in such interviews is available. Generally, child victims should not be interviewed in the home or location where the alleged abuse occurred.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

313.7.2 DETAINING SUSPECTED CHILD ABUSE VICTIMS FOR AN INTERVIEW

A deputy should not detain a child involuntarily who is suspected of being a victim of child abuse solely for the purpose of an interview or physical exam without the consent of a parent or guardian unless one of the following applies:

(a) Exigent circumstances exist, such as:

1. A reasonable belief that medical issues of the child need to be addressed immediately.
2. A reasonable belief that the child is or will be in danger of harm if the interview or physical exam is not immediately completed.
3. The alleged offender is the custodial parent or guardian and there is reason to believe the child may be in continued danger.

(b) A court order or warrant has been issued.

313.7.3 INTERVIEW OF VICTIM OR VICTIM'S SIBLINGS

A deputy may interview any child suspected of being abused or neglected or to any of his/her siblings without the consent of and outside the presence of the parent, guardian or legal custodian of the child (Va. Code § 63.2-1518).

313.8 MEDICAL EXAMINATIONS

If the child has been the victim of abuse that requires a medical examination, the on-call investigator shall be notified. The investigator should obtain consent for such examination from the appropriate parent, guardian or agency having legal custody of the child. The investigator should also arrange for the child's transportation to the appropriate medical facility.

In cases where the alleged offender is the custodial parent or guardian and is refusing consent for the medical examination, the investigator should notify a supervisor before proceeding. If exigent circumstances do not exist or if Commonwealth law does not provide for deputies to take the child for a medical examination, the notified supervisor should consider obtaining a court order for such an examination (Va. Code § 63.2-1524).

313.9 DRUG-ENDANGERED CHILDREN

A coordinated response by law enforcement and social services agencies is appropriate to meet the immediate and longer-term medical and safety needs of children exposed to the manufacturing, trafficking or use of narcotics.

313.9.1 SUPERVISOR RESPONSIBILITIES

The Investigation Division supervisor should:

(a) Work with professionals from the appropriate agencies, including CPS, other law enforcement agencies, medical service providers and local prosecutors to develop community-specific procedures for responding to situations where there are children endangered by their exposure to methamphetamine labs or the manufacture and trafficking of other drugs.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Activate any available interagency response when a deputy notifies the Investigation Division supervisor that the deputy has responded to a drug lab or other narcotics crime scene where a child is present or where evidence indicates that a child lives at the scene.

(c) Develop a report format or checklist for use when deputies respond to drug labs or other narcotics crime scenes. The checklist will help deputies document the environmental, medical, social and other conditions that may affect the child.

313.9.2 DEPUTY RESPONSIBILITIES

Deputies responding to a drug lab or other narcotics crime scene where a child is present or where there is evidence that a child lives should:

(a) Document the environmental, medical, social and other conditions of the child using photography as appropriate and the checklist or form developed for this purpose.

(b) Notify the Investigation Division supervisor so an interagency response can begin.

313.10 STATE MANDATES AND OTHER RELEVANT LAWS

The Commonwealth of Virginia requires or permits the following:

313.10.1 RELEASE OF REPORTS

Information related to incidents of child abuse or suspected child abuse shall be confidential and may only be disclosed pursuant to state law and the Records Maintenance and Release Policy (Va. Code § 63.2-1509).

313.10.2 CHILD FATALITY REVIEW TEAM

The Department shall cooperate fully with state and local child fatality review teams in accordance with Va. Code § 32.1-283.1 and Va. Code § 32.1-283.2.

313.11 TRAINING

The Department should provide training on best practices in child abuse investigations to members tasked with investigating these cases. The training should include:

(a) Participating in multidisciplinary investigations, as appropriate.

(b) Conducting forensic interviews.

(c) Availability of therapy services for children and families.

(d) Availability of specialized forensic medical exams.

(e) Cultural competence (including interpretive services) related to child abuse investigations.

(f) Availability of victim advocate or guardian ad litem support.

(g) Recognizing abuse that requires mandatory notification to another agency.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Adult Abuse

314.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the investigation and reporting of suspected abuse of certain adults who may be more vulnerable than others. This policy also addresses mandatory notification for Madison County Sheriff's Office members as required by law.

314.1.1 DEFINITIONS

Definitions related to this policy include:

Adult abuse - Any offense or attempted offense involving violence or neglect of an adult victim when committed by a person responsible for the adult's care, or any other act that would mandate reporting or notification to a social service agency or law enforcement.

314.2 POLICY

The Madison County Sheriff's Office will investigate all reported incidents of alleged adult abuse and ensure proper reporting and notification as required by law (Va. Code § 63.2-1606).

314.3 MANDATORY NOTIFICATION

Members of the Madison County Sheriff's Office shall notify Adult Protective Services (APS) when a member has reason to believe that a qualifying adult has been the victim of abuse, neglect or exploitation (Va. Code § 63.2-1606; 22 VAC 30-100-15).

For purpose of notification, a qualifying adult is a person 60 years of age or older, or any person 18 years of age or older who is impaired by reason of mental illness, intellectual disability, physical illness or disability, or other causes to the extent that the adult lacks sufficient understanding or capacity to make, communicate or carry out responsible decisions concerning his/her well-being. Abuse means the willful infliction of pain, injury or mental anguish, or unreasonable confinement. Exploitation means the illegal, unauthorized, improper or fraudulent use of a qualifying adult or his/her funds, property, benefits, resources or other assets for profit, benefit or advantage (Va. Code § 63.2-100; Va. Code § 63.2-1603; 22 VAC 30-100-10).

314.3.1 NOTIFICATION PROCEDURE

Notification should occur as follows (Va. Code § 63.2-1606):

(a) Notification shall be made as soon as practicable.

(b) Notification should include specific information as to the adult's location and contact information.

(c) The notification should describe the circumstances of the alleged abuse, neglect or exploitation.

314.4 QUALIFIED INVESTIGATORS

Qualified investigators should be available to investigate cases of adult abuse. These investigators should:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) Conduct interviews in appropriate interview facilities.

(b) Be familiar with forensic interview techniques specific to adult abuse investigations.

(c) Present all cases of alleged adult abuse to the prosecutor for review.

(d) Coordinate with other enforcement agencies, social service agencies and facility administrators as needed.

(e) Provide referrals to therapy services, victim advocates, guardians and support for the victim and family as appropriate.

(f) Participate in or coordinate with multidisciplinary investigative teams as applicable.

(g) When so assigned, assist an adult fatality review team with their investigation of a related death (Va. Code § 32.1-283.5; Va. Code § 32.1-283.6).

314.5 INVESTIGATIONS AND REPORTING

All reported or suspected cases of adult abuse require investigation and a report, even if the allegations appear unfounded or unsubstantiated.

Investigations and reports related to suspected cases of adult abuse should address, as applicable:

(a) The overall basis for the contact. This should be done by the investigating deputy in all circumstances where a suspected adult abuse victim is contacted.

(b) Any relevant statements the victim may have made and to whom he/she made the statements.

(c) If a person is taken into protective custody, the reasons, the name and title of the person making the decision, and why other alternatives were not appropriate.

(d) Documentation of any visible injuries or any injuries identified by the victim. This should include photographs of such injuries, if practicable.

(e) Whether the victim was transported for medical treatment or a medical examination.

(f) Whether the victim identified a household member as the alleged perpetrator, and a list of the names of any other potential victims or witnesses who may reside in the residence.

(g) Identification of any prior related reports or allegations of abuse, including other jurisdictions, as reasonably known.

(h) Previous addresses of the victim and suspect.

(i) Other potential witnesses who have not yet been interviewed, such as relatives or others close to the victim’s environment.

Any unexplained death of an adult who was in the care of a guardian or caretaker should be considered as potential adult abuse and investigated similarly.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

314.6 PROTECTIVE CUSTODY

Before taking an adult abuse victim into protective custody when facts indicate the adult may not be able to care for him/herself, the deputy should make reasonable attempts to contact APS. Generally, removal of an adult abuse victim from his/her family, guardian or other responsible adult should be left to the welfare authorities when they are present or have become involved in an investigation.

Generally, members of this department should remove an adult abuse victim from his/her family or guardian without a court order only when no other effective alternative is reasonably available and immediate action reasonably appears necessary to protect the victim. Prior to taking an adult abuse victim into protective custody, the deputy should take reasonable steps to deliver the adult to another qualified legal guardian, unless it reasonably appears that the release would endanger the victim or result in abduction. If this is not a reasonable option, the deputy shall ensure that the adult is delivered to APS.

Whenever practicable, the deputy should inform a supervisor of the circumstances prior to taking an adult abuse victim into protective custody. If prior notification is not practicable, deputies should contact a supervisor promptly after taking the adult into protective custody.

Deputies may request physicians and APS members consider applying for a protective order under Va. Code § 37.2-1103 or Va. Code § 63.2-1609.

When adult abuse victims are under state control, have a state-appointed guardian or there are other legal holdings for guardianship, it may be necessary or reasonable to seek a court order on behalf of the adult victim to either remove the adult from a dangerous environment (protective custody) or restrain a person from contact with the adult.

314.7 INTERVIEWS

314.7.1 PRELIMINARY INTERVIEWS

Absent extenuating circumstances or impracticality, deputies should audio record the preliminary interview with a suspected adult abuse victim. Deputies should avoid multiple interviews with the victim and should attempt to gather only the information necessary to begin an investigation. When practicable, investigating deputies should defer interviews until a person who is specially trained in such interviews is available.

314.7.2 DETAINING VICTIMS FOR INTERVIEWS

A deputy should not detain an adult involuntarily who is suspected of being a victim of abuse solely for the purpose of an interview or physical exam without his/her consent or the consent of a guardian unless one of the following applies:

(a) Exigent circumstances exist, such as:

1. A reasonable belief that medical issues of the adult need to be addressed immediately.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. A reasonable belief that the adult is or will be in danger of harm if the interview or physical exam is not immediately completed.

3. The alleged offender is a family member or guardian and there is reason to believe the adult may be in continued danger.

(b) A court order or warrant has been issued.

314.8 MEDICAL EXAMINATIONS

When an adult abuse investigation requires a medical examination, the investigating deputy should obtain consent for such examination from the victim, guardian, agency or entity having legal custody of the adult. See attachment: 314 HIPAA Compliant Medical Records Release Form.pdf. The deputy should also arrange for the adult's transportation to the appropriate medical facility.

In cases where the alleged offender is a family member, guardian, agency or entity having legal custody and is refusing to give consent for the medical examination, deputies should notify a supervisor before proceeding. If exigent circumstances do not exist or if state law does not provide for deputies to take the adult for a medical examination, the supervisor should consider other government agencies or services that may obtain a court order for such an examination.

314.9 DRUG-ENDANGERED VICTIMS

A coordinated response by law enforcement and social services agencies is appropriate to meet the immediate and longer-term medical and safety needs of an adult abuse victim who has been exposed to the manufacturing, trafficking or use of narcotics.

314.9.1 SUPERVISOR RESPONSIBILITIES

The Investigation Division supervisor should:

(a) Work with professionals from the appropriate agencies, including APS, other law enforcement agencies, medical service providers and local prosecutors to develop community-specific procedures for responding to situations where there are adult abuse victims endangered by exposure to methamphetamine labs or the manufacture and trafficking of other drugs.

(b) Activate any available interagency response when a deputy notifies the Investigation Division supervisor that he/she has responded to a drug lab or other narcotics crime scene where an adult abuse victim is present or where evidence indicates that an adult abuse victim lives at the scene.

(c) Develop a report format or checklist for use when deputies respond to drug labs or other narcotics crime scenes. The checklist will help deputies document the environmental, medical, social and other conditions that may affect the adult. See attachment: 314 Checklist for Drug-Endangered Dependent Persons Investigations.pdf.

314.9.2 DEPUTY RESPONSIBILITIES

Deputies responding to a drug lab or other narcotics crime scene where an adult abuse victim is present or where there is evidence that an adult abuse victim lives should:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) Document the environmental, medical, social and other conditions of the adult, using photography as appropriate and the checklist or form developed for this purpose.

(b) Notify the Investigation Division supervisor so an interagency response can begin.

314.10 STATE MANDATES AND OTHER RELEVANT LAWS

Virginia requires or permits the following:

314.10.1 RECORDS DIVISION RESPONSIBILITIES

The Records Division is responsible for:

(a) Providing a copy of the adult abuse report to APS as required by law.

(b) Retaining the original adult abuse report with the initial case file.

314.10.2 RELEASE OF REPORTS

Information related to incidents of adult abuse or suspected adult abuse shall be confidential and may only be disclosed pursuant to commonwealth law and the Records Maintenance and Release Policy (Va. Code § 63.2-1605; 22 VAC 30-100-50).

314.10.3 POINT OF CONTACT

The Investigation Division supervisor shall establish a point of contact to receive referrals of suspected adult abuse and shall provide the point-of-contact information to the appropriate local office of the Department of Social Services (Va. Code § 63.2-1605).

The point of contact should work with the Investigation Division supervisor to facilitate the receipt, entry, and processing of protective orders involving a qualifying adult, and any subsequent return or communication with the issuing court, as required by Va. Code 63.2-1609.

314.11 TRAINING

The Department should provide training on best practices in adult abuse investigations to members tasked with investigating these cases. The training should include:

(a) Participating in multidisciplinary investigations, as appropriate.

(b) Conducting interviews.

(c) Availability of therapy services for adults and families.

(d) Availability of specialized forensic medical exams.

(e) Cultural competence (including interpretive services) related to adult abuse investigations.

(f) Availability of victim advocates or other support.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Discriminatory Harassment

315.1 PURPOSE AND SCOPE

The purpose of this policy is to prevent department members from being subjected to discriminatory harassment, including sexual harassment and retaliation. Nothing in this policy is intended to create a legal or employment right or duty that is not created by law.

315.2 POLICY

The Madison County Sheriff's Office is an equal opportunity employer and is committed to creating and maintaining a work environment that is free of all forms of discriminatory harassment, including sexual harassment and retaliation. The Department will not tolerate discrimination against a member in hiring, promotion, discharge, compensation, fringe benefits and other privileges of employment. The Department will take preventive and corrective action to address any behavior that violates this policy or the rights and privileges it is designed to protect.

The nondiscrimination policies of the Department may be more comprehensive than state or federal law. Conduct that violates this policy may not violate state or federal law but still could subject a member to discipline.

315.3 DEFINITIONS

Definitions related to this policy include:

315.3.1 DISCRIMINATION

The Department prohibits all forms of discrimination, including any employment-related action by a member that adversely affects an applicant or member and is based on actual or perceived race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, age, disability, pregnancy, genetic information, veteran status, marital status, and any other classification or status protected by law (Va. Code § 2.2-3900).

Discriminatory harassment, including sexual harassment, is verbal or physical conduct that demeans or shows hostility or aversion toward an individual based upon that individual’s protected class. It has the effect of interfering with an individual’s work performance or creating a hostile or abusive work environment.

Conduct that may, under certain circumstances, constitute discriminatory harassment can include making derogatory comments; making crude and offensive statements or remarks; making slurs or off-color jokes; stereotyping; engaging in threatening acts; making indecent gestures, pictures, cartoons, posters, or material; making inappropriate physical contact; or using written material or department equipment and/or systems to transmit or receive offensive material, statements, or pictures. Such conduct is contrary to department policy and to a work environment that is free of discrimination.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

315.3.2 RETALIATION
Retaliation is treating a person differently or engaging in acts of reprisal or intimidation against the person because the person has engaged in protected activity, filed a charge of discrimination, participated in an investigation, or opposed a discriminatory practice. Retaliation will not be tolerated.

315.3.3 SEXUAL HARASSMENT
The Department prohibits all forms of discrimination and discriminatory harassment, including sexual harassment. It is unlawful to harass an applicant or a member because of that person's sex.

Sexual harassment includes but is not limited to unwelcome sexual advances, requests for sexual favors, or other verbal, visual, or physical conduct of a sexual nature when:

(a) Submission to such conduct is made either explicitly or implicitly as a term or condition of employment, position, or compensation.

(b) Submission to, or rejection of, such conduct is used as the basis for any employment decisions affecting the member.

(c) Such conduct has the purpose or effect of substantially interfering with a member's work performance or creating an intimidating, hostile, or offensive work environment.

315.3.4 ADDITIONAL CONSIDERATIONS
Discrimination and discriminatory harassment do not include actions that are in accordance with established rules, principles, or standards, including:

(a) Acts or omission of acts based solely upon bona fide occupational qualifications under the Equal Employment Opportunity Commission guidelines.

(b) Bona fide requests or demands by a supervisor that the member improve the member's work quality or output, that the member report to the job site on time, that the member comply with county or department rules or regulations, or any other appropriate work-related communication between supervisor and member.

315.4 RESPONSIBILITIES
This policy applies to all department members, who shall follow the intent of these guidelines in a manner that reflects department policy, professional standards, and the best interest of the Department and its mission.

Members are encouraged to promptly report any discriminatory, retaliatory, or harassing conduct or known violations of this policy to a supervisor. Any member who is not comfortable with reporting violations of this policy to the member's immediate supervisor may bypass the chain of command and make the report to a higher-ranking supervisor or manager. Complaints may also be filed with the Sheriff.

Any member who believes, in good faith, that the member has been discriminated against, harassed, or subjected to retaliation, or who has observed harassment, discrimination, or retaliation, is encouraged to promptly report such conduct in accordance with the procedures set forth in this policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Supervisors and managers receiving information regarding alleged violations of this policy shall determine if there is any basis for the allegation and shall proceed with a resolution as stated below.

315.4.1 QUESTIONS OR CLARIFICATION

Members with questions regarding what constitutes discrimination, sexual harassment, or retaliation are encouraged to contact a supervisor or the Sheriff for further information, direction, or clarification.

315.4.2 SUPERVISOR RESPONSIBILITIES

The responsibilities of supervisors shall include but are not limited to:

(a) Continually monitoring the work environment and striving to ensure that it is free from all types of unlawful discrimination, including harassment or retaliation.

(b) Taking prompt, appropriate action within their work units to avoid and minimize the incidence of any form of discrimination, harassment, or retaliation.

(c) Ensuring that their subordinates understand their responsibilities under this policy.

(d) Ensuring that members who make complaints or who oppose any unlawful employment practices are protected from retaliation and that such matters are kept confidential to the extent possible.

(e) Making a timely determination regarding the substance of any allegation based upon all available facts.

(f) Notifying the Sheriff in writing of the circumstances surrounding any reported allegations or observed acts of discrimination, harassment, or retaliation no later than the next business day.

315.4.3 SUPERVISOR'S ROLE

Supervisors shall be aware of the following:

(a) Behavior of supervisors should represent the values of the Department and professional standards.

(b) False or mistaken accusations of discrimination, harassment, or retaliation can have negative effects on the careers of innocent members.

Nothing in this section shall be construed to prevent supervisors from discharging supervisory or management responsibilities, such as determining duty assignments, evaluating or counseling members, or issuing discipline in a manner that is consistent with established procedures.

315.5 INVESTIGATION OF COMPLAINTS

Various methods of resolution exist. During the pendency of any such investigation, the supervisor of the involved member should take prompt and reasonable steps to mitigate or eliminate any continuing abusive or hostile work environment. It is the policy of the Department that all complaints of discrimination, retaliation, or harassment shall be fully documented, and promptly and thoroughly investigated.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

315.5.1 SUPERVISOR RESOLUTION

Members who believe they are experiencing discrimination, harassment, or retaliation should be encouraged to inform the individual that the behavior is unwelcome, offensive, unprofessional, or inappropriate. However, if the member feels uncomfortable or threatened or has difficulty expressing the member's concern, or if this does not resolve the concern, assistance should be sought from a supervisor or manager who is a rank higher than the alleged transgressor.

315.5.2 FORMAL INVESTIGATION

If the complaint cannot be satisfactorily resolved through the supervisory resolution process, a formal investigation will be conducted.

The person assigned to investigate the complaint will have full authority to investigate all aspects of the complaint. Investigative authority includes access to records and the cooperation of any members involved. No influence will be used to suppress any complaint and no member will be subject to retaliation or reprisal for filing a complaint, encouraging others to file a complaint, or for offering testimony or evidence in an investigation.

Formal investigation of the complaint will be confidential to the extent possible and will include but is not limited to details of the specific incident, frequency and dates of occurrences, and names of any witnesses. Witnesses will be advised regarding the prohibition against retaliation, and that a disciplinary process, up to and including termination, may result if retaliation occurs.

Members who believe they have been discriminated against, harassed, or retaliated against because of their protected status are encouraged to follow the chain of command but may also file a complaint directly with the Sheriff, the Human Resources Generalist, or the County Administrator.

315.5.3 ALTERNATIVE COMPLAINT PROCESS

No provision of this policy shall be construed to prevent any member from seeking legal redress outside the Department. Members who believe that they have been harassed, discriminated against, or retaliated against are entitled to bring complaints of employment discrimination to federal, state, and/or local agencies responsible for investigating such allegations. Specific time limitations apply to the filing of such charges. Members are advised that proceeding with complaints under the provisions of this policy does not in any way affect those filing requirements.

315.6 DOCUMENTATION OF COMPLAINTS

All complaints or allegations shall be thoroughly documented on the appropriate forms and in a manner designated by the Sheriff. The outcome of all reports shall be:

(a) Approved by the Sheriff.

(b) Maintained in accordance with the established records retention schedule.

See attachment: Report of Discriminatory Harassment.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

315.6.1 NOTIFICATION OF DISPOSITION
The complainant and/or victim will be notified in writing of the disposition of the investigation and the actions taken to remedy or address the circumstances giving rise to the complaint.

315.7 TRAINING

All new members shall be provided with a copy of this policy as part of their orientation. The policy shall be reviewed with each new member. The member shall certify by signing the prescribed form that the member has been advised of this policy, is aware of and understands its contents, and agrees to abide by its provisions during the member's term with the Department.

All members shall receive annual training on the requirements of this policy and shall certify by signing the prescribed form that they have reviewed the policy, understand its contents, and agree that they will continue to abide by its provisions.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Missing Persons

316.1 PURPOSE AND SCOPE

This policy provides guidance for handling missing person investigations.

316.1.1 DEFINITIONS

Definitions related to this policy include:

Missing child - Any person meeting the following criteria (Va. Code § 52-32):

(a) Under the age of 21 years

(b) Whose temporary or permanent residence is in Virginia or is believed to be in Virginia

(c) Whose whereabouts are unknown to any parent, guardian, legal custodian, or other person standing in loco parentis of the child

(d) Who has been reported as missing to a law enforcement agency within the Commonwealth of Virginia

Critically missing adult - Any adult, including an adult who has a developmental or intellectual disability or mental illness, meeting the following criteria (Va. Code § 15.2-1718.2; Va. Code § 52-34.10):

(a) Whose whereabouts are unknown

(b) Whose disappearance indicates a credible threat to the health and safety of the adult as determined by a law enforcement agency and under such other appropriate circumstances

Missing senior adult - Any person meeting the following criteria (Va. Code § 52-34.4):

(a) Over 60 years of age

(b) Whose whereabouts are unknown

(c) Who suffers a cognitive impairment to the extent that the person is unable to provide care to self without assistance from a caregiver, including a diagnosis of Alzheimer's disease or dementia, and whose disappearance poses a credible threat to the person's health and safety, as determined by a law enforcement agency

(d) Whose disappearance meets other circumstances as deemed appropriate by the Virginia State Police

Missing person with autism - Any person meeting the following criteria (Va. Code § 52-34.13):

(a) Whose whereabouts are unknown

(b) Who has been diagnosed with autism spectrum disorder as defined in Va. Code § 38.2-3418.17

(c) Whose disappearance indicates a credible threat to the health and safety of the person as determined by a law enforcement agency and under such other circumstances deemed appropriate by the Virginia State Police

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

At risk - Includes persons who:

(a) Are 13 years of age or younger.

(b) Regardless of age, are believed or determined to be experiencing one or more of the following circumstances:

1. Out of the zone of safety for their chronological age and developmental stage.
2. Mentally or behaviorally disabled.
3. Drug dependent, including prescribed medication and/or illegal substances, and the dependency is potentially life-threatening.
4. Absent from home for more than 24 hours before being reported to law enforcement as missing.
5. In a life-threatening situation.
6. In the company of others who could endanger their welfare.
7. Absent in a way that is inconsistent with established patterns of behavior and cannot be readily explained. Most children have an established and reasonably predictable routine.
8. Involved in a situation that would cause a reasonable person to conclude the person should be considered at risk.

(c) Qualify for a state AMBER Alert™ pursuant to Va. Code § 52-34.1 et seq.

Missing person - Any person who is reported missing to law enforcement when that person's location is unknown.

Missing person networks - Databases or computer networks that are available to law enforcement and are suitable for obtaining information related to missing person investigations. This includes the National Crime Information Center (NCIC), the Virginia Criminal Information Network (VCIN), and the Missing Children Information Clearinghouse (MCIC) (Va. Code § 15.2-1718).

316.2 POLICY

The Madison County Sheriff's Office does not consider any report of a missing person to be routine and assumes that the missing person is in need of immediate assistance until an investigation reveals otherwise. Priority shall be given to missing person cases over property-related cases. Members will initiate an investigation into all reports of missing persons, regardless of the length of time the person has been missing.

316.3 REQUIRED FORMS AND BIOLOGICAL SAMPLE COLLECTION KITS

The Investigation Division supervisor shall ensure the following forms and kits are developed and available:

- Missing person report form

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

- Missing person investigation checklist that provides investigation guidelines and resources that could be helpful in the early hours of a missing person investigation
- Missing person school notification form
- Medical records release form
- Biological sample collection kits

See attachment: SP-067_Va_Missing_Adult_Info_Clearinghouse_Report.pdf

See attachment: SP-183_Va_Missing_Children_Info_Clearinghouse_Report.pdf

See attachment: 316 Investigative checklist for Missing Children.pdf

See attachment: 316 Missing Persons Investigation Checklist.pdf

See attachment: 316 Missing Child School Notification Form.pdf

See attachment: 316 HIPAA Compliant Medical Records Release Form.pdf

316.4 ACCEPTANCE OF REPORTS

Any member encountering an individual who wishes to report a missing person or runaway shall render assistance without delay. This can be accomplished by accepting the report via telephone or in-person and initiating the investigation. Those members who do not take such reports or who are unable to give immediate assistance shall promptly dispatch or alert a member who can take the report.

A report shall be accepted in all cases and regardless of where the person was last seen, where the person resides or any question of jurisdiction.

316.5 INITIAL INVESTIGATION

Deputies or other members conducting the initial investigation of a missing person should take the following investigative actions, as applicable:

(a) Respond to a dispatched call as soon as practicable.

(b) Interview the reporting party and any witnesses to determine whether the person qualifies as a missing person and, if so, whether the person may be at risk.

(c) Notify a supervisor immediately if there is evidence that a missing person is either at risk or may qualify for a public alert, or both (see the Public Alerts Policy).

(d) Broadcast an alert if the person is a missing senior adult, critically missing adult, missing person with autism, is under 21 years of age, or there is evidence that the missing person is at risk. The alert should be broadcast as soon as practicable but in no event more than two hours after determining the missing person is a missing senior adult, is a critically missing adult, is under 21 years of age, or may be at risk.

(e) Ensure that entries are made into the appropriate missing person networks (Va. Code § 15.2-1718; Va. Code § 15.2-1718.1; Va. Code § 15.2-1718.2; 34 USC § 41308):

1. Immediately, when the missing person is at risk

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. In all other cases, as soon as practicable, but not later than two hours from the time of the initial report.

(f) Complete the appropriate report forms accurately and completely, including but not limited to missing person report, missing person with autism report, critically missing adult report, or missing senior adult report forms, and initiate a search as applicable under the facts.

(g) Collect and/or review:

(a) A photograph and fingerprint card of the missing person, if available.

(b) A voluntarily provided biological sample of the missing person, if available (e.g., toothbrush, hairbrush).

(c) Any documents that may assist in the investigation, such as court orders regarding custody.

(d) Any other evidence that may assist in the investigation, including personal electronic devices (e.g., cell phones, computers).

(h) When circumstances permit and if appropriate, attempt to determine the missing person's location through his/her telecommunications carrier (Va. Code § 19.2-70.2; Va. Code § 19.2-70.3).

(i) Contact the appropriate agency if the report relates to a missing person report previously made to another agency and that agency is actively investigating the report. When this is not practicable, the information should be documented in an appropriate report for transmission to the appropriate agency. If the information relates to an at-risk missing person, the member should notify a supervisor and proceed with reasonable steps to locate the missing person.

316.6 REPORT PROCEDURES AND ROUTING

Members should complete all missing person reports and forms promptly and advise the appropriate supervisor as soon as a missing person report is ready for review.

316.6.1 SUPERVISOR RESPONSIBILITIES

The responsibilities of the supervisor shall include, but are not limited to:

(a) Reviewing and approving missing person reports upon receipt.

1. The reports should be promptly sent to the Records Division.

(b) Ensuring resources are deployed as appropriate.

(c) Initiating a command post as needed.

(d) Ensuring applicable notifications and public alerts are made and documented.

(e) Ensuring that records have been entered into the appropriate missing person networks.

(f) Taking reasonable steps to identify and address any jurisdictional issues to ensure cooperation among agencies.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1. If the case falls within the jurisdiction of another agency, the supervisor should facilitate transfer of the case to the agency of jurisdiction.

316.6.2 RECORDS DIVISION RESPONSIBILITIES

The responsibilities of the Records Division receiving member shall include but are not limited to:

(a) As soon as reasonable under the circumstances, notifying and forwarding a copy of the report to the agency of jurisdiction for the missing person's residence in cases where the missing person is a resident of another jurisdiction.

(b) Notifying and forwarding a copy of the report to the agency of jurisdiction where the missing person was last seen.

(c) Notifying and forwarding a copy of the report to the agency of jurisdiction for the missing person's intended or possible destination, if known.

(d) Forwarding a copy of the report to the Investigation Division.

(e) Coordinating with the NCIC Terminal Contractor for Virginia to have the missing person record in the NCIC computer networks updated with additional information obtained from missing person investigations (34 USC § 41308).

316.7 INVESTIGATION DIVISION FOLLOW-UP

In addition to completing or continuing any actions listed above, the investigator assigned to a missing person investigation:

(a) Shall ensure that the missing person's school is notified within 24 hours or the next business day if the missing person is a missing child (Va. Code § 52-31.1).

1. The notice shall be in writing and should also include a photograph.

2. The investigator should meet with school officials as appropriate to stress the importance of including the notice in the child's student file, along with the investigator's contact information, if the school receives a call requesting the transfer of the missing child's files to another school.

3. The investigator shall notify the appropriate school of the child's status and request tagging of the missing child's file and reporting to this department, and to any other requesting agency, of the child's status.

(b) Should recontact the reporting party and/or other witnesses within 30 days of the initial report and within 30 days thereafter to keep them informed, as appropriate, and to determine if any additional information has become available.

(c) Should consider contacting other agencies involved in the case to determine if any additional information is available.

(d) Shall verify and update VCIN, MCIC, and NCIC and any other applicable missing person networks within 30 days of the original entry into the networks and every 30 days thereafter until the missing person is located (34 USC § 41308).

(e) Should continue to make reasonable efforts to locate the missing person and document these efforts at least every 30 days.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(f) Shall maintain a close liaison with state and local child welfare systems and the National Center for Missing and Exploited Children (NCMEC) if the missing person is under the age of 21 and shall promptly notify NCMEC when the person is missing from a foster care family home or childcare institution (34 USC § 41308).

(g) Should make appropriate inquiry with the Medical Examiner.

(h) Should obtain and forward medical and dental records, photos, X-rays, and biological samples, as applicable.

(i) Should attempt to obtain the most recent photograph for persons under 18 years of age if it has not been obtained previously and forward the photograph to VCIN or MCIC and enter the photograph into applicable missing person networks (34 USC § 41308).

(j) Should consider making appropriate entries and searches in the National Missing and Unidentified Persons System (NamUs).

(k) In the case of an at-risk missing person or a person who has been missing for an extended time, should consult with a supervisor regarding seeking federal assistance from the FBI and the U.S. Marshals Service (28 USC § 566).

316.8 WHEN A MISSING PERSON IS FOUND

When any person reported missing is found, the assigned investigator shall document the location of the missing person in the appropriate report, notify the relatives and/or reporting party, as appropriate, and other involved agencies, and refer the case for additional investigation if warranted. When a missing child is found, notification shall be promptly made to all involved agencies as provided in Va. Code § 52-34.

The Records Manager shall ensure that, upon receipt of information that a missing person has been located, the following occurs:

(a) Notification is made to VCIN, MCIC, and NCIC.

(b) The missing child’s school is notified.

(c) Entries are made in the applicable missing person networks.

(d) When a person is a missing child or at risk, the fact that the person has been found shall be reported immediately to MCIC and VCIN (Va. Code § 52-34).

(e) Notification shall be made to any other law enforcement agency that took the initial report or participated in the investigation.

316.8.1 UNIDENTIFIED PERSONS

Members investigating a case of an unidentified person who is deceased or a living person who cannot assist in identifying him/herself should:

(a) Obtain a complete description of the person.

(b) Enter the unidentified person’s description into the NCIC Unidentified Person File.

(c) Use available resources, such as those related to missing persons, to identify the person.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

316.9 CASE CLOSURE

The Investigation Division supervisor may authorize the closure of a missing person case after considering the following:

(a) Closure is appropriate when the missing person is confirmed returned or evidence matches an unidentified person or body.

(b) If the missing person is a resident of Madison County, Virginia or this department is the lead agency, the case should be kept under active investigation for as long as the person may still be alive. Exhaustion of leads in the investigation should not be a reason for closing a case.

(c) If this department is not the lead agency, the case can be made inactive if all investigative leads have been exhausted, the lead agency has been notified and entries are made in the applicable missing person networks, as appropriate.

(d) A missing person case should not be closed or reclassified because the person would have reached a certain age or adulthood or because the person is now the subject of a criminal or civil warrant.

316.10 TRAINING

Subject to available resources, the Training Supervisor should ensure that members of this department whose duties include missing person investigations and reports receive training that includes:

(a) The initial investigation:

1. Assessments and interviews
2. Use of current resources, such as Mobile Audio/Video (MAV)
3. Confirming missing status and custody status of minors
4. Evaluating the need for a heightened response
5. Identifying the zone of safety based on chronological age and developmental stage

(b) Briefing of department members at the scene.

(c) Identifying NCIC Missing Person File categories (e.g., disability, endangered, involuntary, juvenile and catastrophe).

(d) Verifying the accuracy of all descriptive information.

(e) Initiating a neighborhood investigation.

(f) Investigating any relevant recent family dynamics.

(g) Addressing conflicting information.

(h) Key investigative and coordination steps.

(i) Managing a missing person case.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(j) Additional resources and specialized services.

(k) Update procedures for case information and descriptions.

(l) Preserving scenes.

(m) Internet and technology issues (e.g., Internet use, cell phone use).

(n) Media relations.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Public Alerts

317.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for alerting the public to important information and soliciting public aid when appropriate.

317.2 POLICY

Public alerts may be employed using the Emergency Alert System (EAS), local radio, television and press organizations and other groups to notify the public of incidents, or enlist the aid of the public, when the exchange of information may enhance the safety of the community. Various types of alerts may be available based upon each situation and the alert system's individual criteria.

317.3 RESPONSIBILITIES

317.3.1 MEMBER RESPONSIBILITIES

Members of the Madison County Sheriff's Office should notify their supervisors, Shift Supervisor or Investigation Division supervisor as soon as practicable upon learning of a situation where public notification, a warning or enlisting the help of the media and the public could assist in locating a missing person, apprehending a dangerous person or gathering information.

317.3.2 SUPERVISOR RESPONSIBILITIES

A supervisor apprised of the need for a public alert is responsible for making the appropriate notifications based upon the circumstances of each situation. The supervisor shall promptly notify the Sheriff, the appropriate Division Supervisor and the Public Information Officer when any public alert is generated.

The supervisor in charge of the investigation to which the alert relates is responsible for:

(a) Updating alerts.

(b) Canceling alerts.

(c) Ensuring all appropriate reports are completed.

(d) Preparing an after-action evaluation of the investigation to be forwarded to the Division Supervisor.

317.4 AMBER ALERTS™

AMBER Alerts™ are used to provide a statewide system for the rapid dissemination of information regarding abducted children.

317.4.1 CRITERIA

The following criteria are utilized to determine if an AMBER Alert should be requested (Va. Code § 52-34.3):

(a) The victim of the abduction is a child less than 18 years of age or currently enrolled in a secondary school in the Commonwealth of Virginia.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) A deputy has a reasonable belief that an abduction has occurred.

(c) A deputy believes that the victim is in imminent danger of serious bodily injury or death.

(d) Sufficient information exists about the victim and the suspect for this department to request that the Virginia State Police (VSP) issue an AMBER Alert.

(e) The child must be entered into the Virginia Criminal Information Network (VCIN) and the National Crime Information Center (NCIC) missing person files as soon as practical.

317.4.2 PROCEDURE

Members initiating an AMBER Alert shall (Va. Code § 52-34.3):

(a) Notify all on-duty deputies of the existence of a missing child report.

(b) Ensure that the missing child is entered into the Virginia Criminal Information Network (VCIN) and the National Crime Information Center (NCIC) missing person files as soon as practicable.

(c) Transmit the report to the VSP Administrative Headquarters to request activation of the AMBER Alert system using the approved form.

(d) Confer with the VSP to determine whether the alert should be local, regional or statewide.

(e) Immediately notify the VSP if the missing child is located.

317.5 BLUE ALERTS™

Blue Alerts™ are used to provide a statewide system for the rapid dissemination of information regarding a violent criminal who has seriously injured or killed a local, state or federal law enforcement officer. A Blue Alert can also be activated when a law enforcement officer is missing in the line of duty under circumstances that cause concern for his/her safety (Va. Code § 52-34.8).

317.5.1 CRITERIA

The following criteria are utilized to determine if a Blue Alert should be requested (Va. Code § 52-34.8; Va. Code § 52-34.9):

(a) A law enforcement officer has been killed or seriously injured while in the line of duty.

(b) The suspect has not been apprehended and may be a serious threat to the public or other law enforcement personnel.

(c) Sufficient information is available to disseminate to the public that could assist in locating the suspect.

(d) If a law enforcement officer is missing in the line of duty, sufficient information is available to disseminate to the public that could assist in locating the law enforcement officer.

317.5.2 PROCEDURE

Members initiating a Blue Alert shall (Va. Code § 52-34.9):

(a) Verify that the criteria for activating the Blue Alert has been met.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Notify the VSP and request activation of a Blue Alert.

(c) Immediately notify the VSP if the suspect or the missing law enforcement officer is located.

317.6 SENIOR ALERTS

Senior Alerts are used to provide a statewide system for the rapid dissemination of information regarding a missing senior adult who is over 60 years of age and suffers a cognitive impairment to the extent that he/she is unable to provide care for him/herself without assistance from a caregiver, including a diagnosis of Alzheimer's disease or dementia, and whose disappearance poses a credible threat to his/her health and safety as determined by this department or the VSP (Va. Code § 52-34.4; Va. Code § 52-34.5).

317.6.1 CRITERIA

The following criteria are utilized to determine if a Senior Alert should be requested (Va. Code § 52-34.6):

(a) A deputy believes that a missing senior adult's whereabouts are unknown.

(b) A deputy believes that the missing senior adult is in danger of serious bodily harm at risk of injury or death.

(c) The Madison County Sheriff's Office confirms that an investigation has taken place verifying the disappearance and eliminating alternative explanations for the missing senior adult's disappearance.

(d) Sufficient information regarding the missing senior adult is available to disseminate to the public that could assist in locating the missing senior adult.

317.6.2 PROCEDURE

Members initiating a Senior Alert shall (Va. Code § 52-34.6):

(a) Complete the Virginia Senior Alert forms and forward to the VSP.

(b) Confer with the VSP to determine whether the alert should be local, regional or statewide.

(c) Forward the most current photograph of the missing senior adult to the VSP.

(d) Notify the VSP by telephone and confirm receipt of the forms. The VSP will contact any broadcast companies to activate the Senior Alert.

(e) Enter the missing senior adult into the VCIN and NCIC missing person files as soon as practicable.

(f) Immediately notify the VSP if the missing senior adult is located.

317.7 CRITICALLY MISSING ADULT ALERTS

Critically Missing Adult Alerts are used to provide a system for the rapid dissemination of information regarding missing adults believed to be in imminent danger (Va. Code § 52-34.10 et seq.).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

317.7.1 CRITERIA
The following criteria are utilized to determine if a Critically Missing Adult Alert should be requested (Va. Code § 52-34.10):

(a) There is reason to believe the adult is in imminent danger of serious bodily harm or death.

(b) An investigation has been conducted to verify these and any additional criteria established by the VSP.

(c) There is sufficient information available to disseminate to the public that could assist in locating the missing adult, suspect, or the suspect's vehicle.

317.7.2 PROCEDURE
Members initiating a Critically Missing Adult Alert shall (Va. Code § 52-34.12):

(a) Contact the Virginia State Police to determine whether a local, regional, or statewide alert is appropriate and provide any information that may assist in the safe recovery of the critically missing adult.

(b) Complete the Virginia Critically Missing Adult Alert forms and forward to the VSP.

(c) Enter the critically missing adult into the Virginia Criminal Information Network and the National Crime Information Center.

(d) Follow the procedures established by the VSP for issuing the alert.

317.8 MISSING PERSON WITH AUTISM ALERTS

A Missing Person with Autism Alert is used to provide a system for the rapid dissemination of information regarding a missing person with autism whose disappearance poses a credible threat to the person’s health and safety as determined by this department or the VSP (Va. Code § 52-34.13, et seq.).

317.8.1 CRITERIA
The following criteria are utilized to determine if a Missing Person with Autism Alert should be requested (Va. Code § 52-34.13, et seq.):

(a) There is reason to believe that the whereabouts of a person are unknown.

(b) The person has been diagnosed with autism spectrum disorder as defined in Va. Code § 38.2-3418.17.

(c) There is a credible threat to the health and safety of the person as determined by the Department or other circumstances deemed appropriate by the VSP are satisfied.

(d) An investigation has been conducted that verified the disappearance or eliminated alternative explanations.

(e) There is sufficient information available to disseminate to the public that could assist in locating the missing person.

317.8.2 PROCEDURE
Any member initiating a Missing Person with Autism Alert shall (Va. Code § 52-34.15):

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) Contact the VSP to determine whether a local, regional, or statewide alert is appropriate and provide any information that may assist in the safe recovery of the missing person with autism.

(b) Complete all required forms.

(c) Enter the missing person into the Virginia Criminal Information Network and the National Crime Information Center.

(d) Follow the procedures established by the VSP for issuing the alert.

See attachment: 317 DOJ Amber Alert Field Guide for Law Enforcement Officers.pdf

See attachment: 317 Virginia AMBER Alert Plan (Rev. 3-1-21).pdf

See attachment: 317 Virginia Ashanti Alert - Abducted Adult - Plan.pdf

See attachment: 317 Virginia Ashanti Alert - Abducted Adult - Activation Request Form.pdf

See attachment: 317 Virginia Ashanti Alert - Abducted Adult - Termination Fax Form.pdf

See attachment: 317 Virginia Missing Child With Autism Alert Plan User Guide.pdf

See attachment: 317 Virginia Missing Child with Autism Agency Activation Request Form.pdf

See attachment: 317 Virginia Missing Child with Autism Agency Termination Request Form.pdf

See attachment: 317 Virginia Senior Alert Plan - User Guide.pdf

See attachment: 317 Virginia Senior Alert Request Form.pdf

See attachment: 317 Virginia Senior Alert Termination Fax Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Victim and Witness Assistance

318.1 PURPOSE AND SCOPE

The purpose of this policy is to ensure that crime victims and witnesses receive appropriate assistance, that they are provided with information from government and private resources, and that the agency meets all related legal mandates.

See attachment: VA Madison County SO - Victim Witness Agreement.pdf

318.2 POLICY

The Madison County Sheriff's Office is committed to providing guidance and assistance to the victims and witnesses of crime. The members of the Madison County Sheriff's Office will show compassion and understanding for victims and witnesses and will make reasonable efforts to provide the support and information identified in this policy.

318.3 VICTIM WITNESS SERVICES DIRECTOR

Madison County has appointed a Victim Witness Services Director to help in understanding the court process, developing victim impact statements, and ensuring prosecutors and law enforcement know vital information. The County Victim Witness Services Director will be the point of contact for individuals requiring further assistance or information from the Madison County Sheriff's Office regarding benefits from crime victim resources. This person shall also be responsible for maintaining compliance with all legal mandates related to crime victims and/or witnesses.

318.3.1 VICTIM WITNESS SERVICES DIRECTOR DUTIES

The Victim Witness Services Director or the authorized designee, in consultation with the Investigation Division Division Supervisor, should establish procedures for receiving requests for assistance in applying for U visa or T visa status and make those procedures publicly available for victims, witnesses, and their representatives (Va. Code § 9.1-1501). Those procedures should provide for responses to these requests to be made in compliance with applicable law and as set forth in the Immigration Violations Policy (Va. Code § 9.1-1501).

318.4 CRIME VICTIMS

Deputies should provide all victims with the applicable victim information handouts.

Deputies should never guarantee a victim’s safety from future harm but may make practical safety suggestions to victims who express fear of future harm or retaliation. Deputies should never guarantee that a person qualifies as a victim for the purpose of compensation or restitution but may direct him/her to the proper written department material or available victim resources.

318.5 VICTIM INFORMATION

The Administration Division Supervisor shall ensure that victim information handouts are available and current. These should include preprinted information prepared by the Virginia Department of Criminal Justice Services (DCJS) and, as appropriate:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) Shelters and other community resources for victims of sexual assault or domestic and family violence (Va. Code § 9.1-1301; Va. Code § 19.2-81.3).

(b) Assurance that crime victims will not incur out-of-pocket expenses for forensic medical exams, and information about evidence collection, storage, and preservation in sexual assault cases (34 USC § 10449; 34 USC § 20109; Va. Code § 19.2-165.1; Va. Code § 19.2-11.11; Va. Code § 19.2-11.12).

(c) An advisement that a person who was arrested may be released on bond or some other form of release and that the victim should not rely upon an arrest as a guarantee of safety.

(d) A clear explanation of relevant court orders and how they can be obtained.

1. This should include information regarding the online I-CAN!™ Virginia system that provides assistance with the preparation of court forms required to be filed for a protective order.

(e) Information regarding available compensation for qualifying victims of crime (Va. Code § 19.2-368.1 et seq.).

(f) VINE® information (Victim Information and Notification Everyday), including the telephone number and whether this free service is available to allow victims to check on an offender's custody status and to register for automatic notification when a person is released from jail (Va. Code § 53.1-133.02).

(g) Notice regarding U visa and T visa application processes.

(h) Resources available for victims of identity theft.

(i) Notice that it is unlawful for an employer to penalize an employee for appearing in court pursuant to a summons or subpoena (Va. Code § 18.2-465.1).

(j) A place for the deputy's name, badge number, and any applicable case or incident number, along with a telephone number the victim may call to report additional information about the case or to receive information about the status of the case.

(k) Notice that the Department will withhold, upon request, the address, telephone number, email address, and place of employment of the victim or a member of the victim's family (Va. Code § 19.2-11.2).

(l) An explanation of the rights afforded to victims under the Crime Victim and Witness Rights Act (Va. Code § 19.2-11.01).

(m) Information found in the Bill of Rights for victims (Va. Const. art. I, § 8-A).

(n) Legal resources available to victims of sexual assault (Va. Code § 9.1-1301).

(o) For victims of sexual assault, notice of their right to be kept informed about the submission, testing, and storage of biological evidence (Va. Code § 19.2-11.01; Va. Code § 19.2-11.11).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

318.6 WITNESSES

Deputies should never guarantee a witness' safety from future harm or that his/her identity will always remain confidential. Deputies may make practical safety suggestions to witnesses who express fear of future harm or retaliation.

Deputies should investigate allegations of witness intimidation and take enforcement action when lawful and reasonable.

318.7 WITNESS INFORMATION

The Administration Division Supervisor shall ensure that witness information handouts are available and current. These should include preprinted information prepared by the DCJS and, as appropriate (Va. Code § 19.2-11.01):

(a) Notice that the Department will withhold, upon request, the address, telephone number, email address, and place of employment of the witness or a member of the witness's family (Va. Code § 19.2-11.2).

(b) An explanation of the rights afforded to witnesses under the Crime Victim and Witness Rights Act (Va. Code § 19.2-11.01).

(c) Information regarding the Witness Protection Program (Va. Code § 52-35).

(d) Contact information for local witness programs.

(e) Information regarding medical services, compensation programs, counseling, legal services, or other applicable services.

(f) Information advising witnesses what to do if they are threatened or otherwise intimidated by the suspect or anyone associated with the suspect.

(g) The case number and subsequent steps in the processing of the case.

(h) The telephone number that witnesses may call to report additional information about the case or to receive information about the status of the case.

318.8 POST-INVESTIGATION VICTIM AND WITNESS ASSISTANCE

The Department should ensure victim and witness assistance services are provided during any follow-up investigation, including but not limited to:

(a) Complying with the provisions of state crime victims' compensation statutes.

(b) Complying with all statutory provisions with respect to victims of sex offenses.

(c) Explaining to victims and/or witnesses the procedures involved in their case and their role in those procedures unless detrimental to the prosecution of the case.

(d) Conducting follow-up investigative steps such as scheduling line-ups, interviews, and other required appearances at the convenience of the victim/witness when feasible and providing transportation when required by law, or when the Department deems practicable when not required by law.

(e) Returning victim and witness property when permitted by law or rules of evidence in accordance with the Property and Evidence Section Policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

318.9 DISTRIBUTION OF INFORMATION

Members shall provide information referenced in this policy to victims and witnesses as appropriate during preliminary and follow-up investigations.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Hate Crimes

319.1 PURPOSE AND SCOPE

The purpose of this policy is to provide members of this department with guidelines for identifying and investigating incidents and crimes that may be motivated by hatred or other bias.

319.1.1 DEFINITIONS

Definitions related to this policy include:

Hate crime - A crime motivated by prejudice based on actual or perceived race, color, religion, national origin, ethnicity, gender, sexual orientation, gender identity or expression, or disability of the victim. This includes a crime committed for the purpose of restraining a person from exercising rights under the constitutions or laws of the United States and the Commonwealth (Va. Code § 52-8.5).

319.2 POLICY

The Madison County Sheriff's Office recognizes and places a high priority on the rights of all individuals guaranteed under the state and federal constitution and incorporated in state and federal law.

319.3 PREVENTION AND PREPARATION

While it is recognized that not all crime can be prevented, this department is committed to taking a proactive approach to preventing and preparing for likely hate crimes by:

(a) Making an affirmative effort to establish contact with persons and groups within the community who are likely targets of hate crimes, and forming networks that address prevention and response.

(b) Providing victim assistance and community follow-up or identifying available resources to do so.

(c) Educating community and civic groups about hate crime laws.

319.4 INVESTIGATIONS

Whenever any member of this department receives a report of a suspected hate crime or other activity that reasonably appears to involve a potential hate crime, the following should occur:

(a) Assigned deputies should promptly contact the victim, witness or reporting party to investigate the matter further, as circumstances may dictate.

(b) A supervisor should be notified of the circumstances as soon as practicable.

(c) Once the in-progress aspect of any such situation has been stabilized (e.g., treatment of victims or arrest of suspects at the scene), the assigned deputies should take reasonable steps to preserve evidence that establishes a possible hate crime.

(d) Based upon available information, deputies should take appropriate action to mitigate further injury or damage to potential victims or the community.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(e) Depending on the situation, the assigned deputies or supervisor may request assistance from investigators or other resources.

(f) The assigned deputies should interview available witnesses, victims and others to determine what circumstances, if any, indicate that the situation may involve a hate crime.

(g) The assigned deputies should make reasonable efforts to assist the victim by providing available information on local assistance programs and organizations as required by the Victim and Witness Assistance Policy.

(h) The assigned deputies should include all available evidence indicating the likelihood of a hate crime in the relevant reports. All related reports should be clearly marked "Hate Crime."

(i) The assigned deputies and supervisor should take reasonable steps to ensure that any such situation does not escalate further and should provide information to the victim regarding legal aid (Emergency Protective Order) through the courts or Commonwealth Attorney.

319.4.1 INVESTIGATION DIVISION RESPONSIBILITIES

If a hate crime case is assigned to the Investigation Division, the assigned investigator will be responsible for:

(a) Coordinating further investigation with the Commonwealth Attorney and other appropriate law enforcement agencies.

(b) Maintaining contact with the victim and other involved individuals, as needed.

(c) Maintaining statistical data and tracking of suspected hate crimes, as indicated or required by state law (Va. Code § 52-8.5).

319.5 TRAINING

All members of this department should receive training on hate crime recognition and investigation (6 VAC 20-30-30).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Standards of Conduct

320.1 PURPOSE AND SCOPE

This policy establishes standards of conduct that are consistent with the values and mission of the Madison County Sheriff's Office and are expected of all department members. The standards contained in this policy are not intended to be an exhaustive list of requirements and prohibitions but they do identify many of the important matters concerning conduct. In addition to the provisions of this policy, members are subject to all other provisions contained in this manual, as well as any additional guidance on conduct that may be disseminated by this department or a member's supervisors.

320.2 POLICY

The continued employment or appointment of every member of this department shall be based on conduct that reasonably conforms to the guidelines set forth herein. Failure to meet the guidelines set forth in this policy, whether on- or off-duty, may be cause for disciplinary action.

320.3 DIRECTIVES AND ORDERS

Members shall comply with lawful directives and orders from any department supervisor or person in a position of authority, absent a reasonable and bona fide justification.

320.3.1 UNLAWFUL OR CONFLICTING ORDERS

Supervisors shall not knowingly issue orders or directives that, if carried out, would result in a violation of any law or department policy. Supervisors should not issue orders that conflict with any previous order without making reasonable clarification that the new order is intended to countermand the earlier order.

No member is required to obey any order that appears to be in direct conflict with any federal law, state law or local ordinance. Following a known unlawful order is not a defense and does not relieve the member from criminal or civil prosecution or administrative discipline. If the legality of an order is in doubt, the affected member shall ask the issuing supervisor to clarify the order or shall confer with a higher authority. The responsibility for refusal to obey rests with the member, who shall subsequently be required to justify the refusal.

Unless it would jeopardize the safety of any individual, members who are presented with a lawful order that is in conflict with a previous lawful order, department policy or other directive shall respectfully inform the issuing supervisor of the conflict. The issuing supervisor is responsible for either resolving the conflict or clarifying that the lawful order is intended to countermand the previous lawful order or directive, in which case the member is obliged to comply. Members who are compelled to follow a conflicting lawful order after having given the issuing supervisor the opportunity to correct the conflict will not be held accountable for disobedience of the lawful order or directive that was initially issued.

The person countermanding the original order shall notify, in writing, the person issuing the original order, indicating the action taken and the reason.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

320.3.2 SUPERVISOR RESPONSIBILITIES

Supervisors and managers are required to follow all policies and procedures and may be subject to discipline for:

(a) Failure to be reasonably aware of the performance of their subordinates or to provide appropriate guidance and control.

(b) Failure to promptly and fully report any known misconduct of a member to his/her immediate supervisor or to document such misconduct appropriately or as required by policy.

(c) Directing a subordinate to violate a policy or directive, acquiescing to such a violation or exhibiting indifference to such a violation.

(d) Exercising unequal or disparate authority toward any member for malicious or other improper purpose.

320.4 GENERAL STANDARDS

Members shall conduct themselves, whether on- or off-duty, in accordance with the United States and Virginia constitutions and all applicable laws, ordinances, and rules enacted or established pursuant to legal authority.

Members shall familiarize themselves with policies and procedures and are responsible for compliance with each. Members should seek clarification and guidance from supervisors in the event of any perceived ambiguity or uncertainty.

Discipline may be initiated for any good cause. It is not mandatory that a specific policy or rule violation be cited to sustain discipline. This policy is not intended to cover every possible type of misconduct.

320.5 CAUSES FOR DISCIPLINE

The following are illustrative of causes for disciplinary action. This list is not intended to cover every possible type of misconduct and does not preclude the recommendation of disciplinary action for violation of other rules, standards, ethics and specific action or inaction that is detrimental to efficient department service.

320.5.1 LAWS, RULES AND ORDERS

(a) Violation of, or ordering or instructing a subordinate to violate, any policy, procedure, rule, order, directive or requirement, or failure to follow instructions contained in department or County manuals.

(b) Disobedience of any legal directive or order issued by any department member of a higher rank.

(c) Violation of federal, state, local or administrative laws, rules or regulations.

320.5.2 ETHICS

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) Using or disclosing one's status as a member of the Madison County Sheriff's Office in any way that could reasonably be perceived as an attempt to gain influence or authority for non-department business or activity.

(b) The wrongful or unlawful exercise of authority on the part of any member for malicious purpose, personal gain, willful deceit, or any other improper purpose.

(c) The receipt or acceptance of a reward, fee, or gift from any person for service incident to the performance of the member's duties (lawful subpoena fees and authorized work permits excepted).

(d) Acceptance of fees, gifts, or money contrary to the rules of this department and/or laws of the state.

1. This policy does not prohibit the individual acceptance of occasional, unsolicited gifts, awards, presentations, or honoraria (not cash) when it can be reasonably inferred that the person, business, or organization does not seek to influence any official action for any reason.
2. The Department, or employees on behalf of the Department, may accept reasonable quantities of food and non-alcoholic drinks from citizens or businesses, churches, or other public or private civic organizations offered to the employees of this Department to be shared as a whole as a gesture of appreciation for working nights, weekends, holidays or other special occasions, or during natural or man-made disasters.
3. Employees, with the approval of the Sheriff, may accept invitations to attend, free of charge, a local dinner, event, or outing sponsored or conducted by government or civic organizations.
4. Deputies should obtain the name, address, and telephone number of the individual or organization offering such gifts awards, presentations, or honoraria, and report such information, along with a description of the goods provided to the Sheriff through the chain of command so that the Department is properly able to extend its appreciation.

(e) Offer or acceptance of a bribe or gratuity.

(f) Misappropriation or misuse of public funds, property, personnel, or services.

(g) Any other failure to abide by the standards of ethical conduct.

320.5.3 DISCRIMINATION, OPPRESSION, OR FAVORITISM

Unless required by law or policy, discriminating against, oppressing, or providing favoritism to any person because of actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, age, disability, economic status, cultural group, veteran status, marital status, and any other classification or status protected by law, or intentionally denying or impeding another in the exercise or enjoyment of any right, privilege, power, or immunity, knowing the conduct is unlawful.

320.5.4 RELATIONSHIPS

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) Unwelcome solicitation of a personal or sexual relationship while on-duty or through the use of one's official capacity.

(b) Engaging in on-duty sexual activity including, but not limited to, sexual intercourse, excessive displays of public affection or other sexual contact.

(c) Establishing or maintaining an inappropriate personal or financial relationship, as a result of an investigation, with a known victim, witness, suspect or defendant while a case is being investigated or prosecuted, or as a direct result of any official contact.

(d) Associating with or joining a criminal gang, organized crime and/or criminal syndicate when the member knows or reasonably should know of the criminal nature of the organization. This includes any organization involved in a definable criminal activity or enterprise, except as specifically directed and authorized by this department.

(e) Associating on a personal, rather than official, basis with persons who demonstrate recurring involvement in serious violations of state or federal laws after the member knows, or reasonably should know of such criminal activities, except as specifically directed and authorized by this department.

320.5.5 ATTENDANCE

(a) Leaving the job to which the member is assigned during duty hours without reasonable excuse and proper permission and approval.

(b) Unexcused or unauthorized absence or tardiness.

(c) Excessive absenteeism or abuse of leave privileges.

(d) Failure to report to work or to the place of assignment at the time specified and fully prepared to perform duties without reasonable excuse.

320.5.6 UNAUTHORIZED ACCESS, DISCLOSURE, OR USE

(a) Unauthorized and inappropriate intentional release of confidential or protected information, materials, data, forms, or reports obtained as a result of the member's position with this department.

(b) Disclosing to any unauthorized person any active investigation information.

(c) The use of any information, photograph, video, or other recording obtained or accessed as a result of employment or appointment to this department for personal or financial gain or without the express authorization of the Sheriff or the authorized designee.

(d) Loaning, selling, allowing unauthorized use, giving away, or appropriating any department property for personal use, personal gain, or any other improper or unauthorized use or purpose.

(e) Using department resources in association with any portion of an independent civil action. These resources include but are not limited to personnel, vehicles, equipment, and non-subpoenaed records.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

320.5.7 EFFICIENCY

(a) Neglect of duty.

(b) Unsatisfactory work performance including but not limited to failure, incompetence, inefficiency, or delay in performing and/or carrying out proper orders, work assignments, or the instructions of supervisors without a reasonable and bona fide excuse.

(c) Concealing, attempting to conceal, removing, or destroying defective or incompetent work.

(d) Unauthorized sleeping during on-duty time or assignments.

(e) Failure to notify the Department within 24 hours of any change in residence address or contact numbers.

(f) Failure to notify the Human Resources Department of changes in relevant personal information (e.g., information associated with benefits determination) in a timely fashion.

320.5.8 PERFORMANCE

(a) Failure to disclose or misrepresenting material facts, or making any false or misleading statement on any application, examination form, or other official document, report or form, or during the course of any workrelated investigation.

(b) The falsification of any work-related records, making misleading entries or statements with the intent to deceive, or the willful and unauthorized removal, alteration, destruction and/or mutilation of any department record, public record, book, paper or document.

(c) Failure to participate in investigations, or giving false or misleading statements, or misrepresenting or omitting material information to a supervisor or other person in a position of authority, in connection with any investigation or in the reporting of any department-related business.

(d) Being untruthful or knowingly making false, misleading or malicious statements that are reasonably calculated to harm the reputation, authority or official standing of this department or its members.

(e) Disparaging remarks or conduct concerning duly constituted authority to the extent that such conduct disrupts the efficiency of this department or subverts the good order, efficiency and discipline of this department or that would tend to discredit any of its members.

(f) Unlawful gambling or unlawful betting at any time or any place. Legal gambling or betting under any of the following conditions:

1. While on department premises.
2. At any work site, while onduty or while in uniform, or while using any department equipment or system.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

3. Gambling activity undertaken as part of a deputy's official duties and with the express knowledge and permission of a direct supervisor is exempt from this prohibition.

(g) Improper political activity including:

1. Unauthorized attendance while on--duty at official legislative or political sessions.

2. Solicitations, speeches or distribution of campaign literature for or against any political candidate or position while on-duty, or on department property except as expressly authorized by County policy or the Sheriff (VA Code Ann. § 15.2-1512.2).

(h) Engaging in political activities during assigned working hours except as expressly authorized by County policy or the Sheriff.

(i) Any act on- or off-duty that brings discredit to this department.

320.5.9 CONDUCT

(a) Failure of any member to promptly and fully report activities on his/her part or the part of any other member where such activities resulted in contact with any other law enforcement agency or that may result in criminal prosecution or discipline under this policy.

(b) Unreasonable and unwarranted force to a person encountered or a person under arrest.

(c) Exceeding lawful peace officer powers by unreasonable, unlawful, or excessive conduct.

(d) Unauthorized or unlawful fighting, threatening, or attempting to inflict unlawful bodily harm on another.

(e) Engaging in horseplay that reasonably could result in injury or property damage.

(f) Discourteous, disrespectful, or discriminatory treatment of any member of the public or any member of this department or the County.

(g) Inappropriate use of obscene, indecent, profane, or derogatory language while on-duty or in uniform.

(h) Criminal, dishonest or disgraceful conduct, whether on- or off-duty, that adversely affects the member's relationship with this department.

(i) Unauthorized possession of, loss of, or damage to department property or the property of others, or endangering it through carelessness or maliciousness.

(j) Attempted or actual theft of department property; misappropriation or misuse of public funds, property, personnel, or the services or property of others; unauthorized removal or possession of department property or the property of another person.

(k) Activity that is incompatible with a member's conditions of employment or appointment as established by law or that violates a provision of any County policy, including fraud in securing the appointment or hire.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(l) Initiating any civil action for recovery of any damages or injuries incurred in the course and scope of employment or appointment without first notifying the Sheriff of such action.

(m) Any other on- or off-duty conduct which any member knows or reasonably should know is unbecoming a member of this department, is contrary to good order, efficiency, or morale, or tends to reflect unfavorably upon this department or its members.

320.5.10 SAFETY

(a) Failure to observe or violating department safety standards or safe working practices.

(b) Failure to maintain current licenses or certifications required for the assignment or position (e.g., driver’s license, first aid).

(c) Failure to maintain good physical condition sufficient to adequately and safely perform law enforcement duties.

(d) Unsafe firearm or other dangerous weapon handling including loading or unloading firearms in an unsafe manner, either on- or off-duty.

(e) Carrying, while on the premises of the work site, any firearm or other lethal weapon that is not authorized by the member’s appointing authority.

(f) Unsafe or improper driving habits or actions in the course of employment or appointment.

(g) Any personal action contributing to a preventable traffic accident.

(h) Concealing or knowingly failing to report any on-the-job or work-related accident or injury as soon as practicable but within 24 hours.

320.5.11 INTOXICANTS

(a) Reporting for work or being at work while intoxicated or when the member's ability to perform assigned duties is impaired due to the use of alcohol, medication or drugs, whether legal, prescribed or illegal.

(b) Possession or use of alcohol at any work site or while on-duty, except as authorized in the performance of an official assignment. A member who is authorized to consume alcohol is not permitted to do so to such a degree that it may impair on-duty performance. In no event shall a member report for duty if they have consumed alcohol within the past eight hours.

(c) Unauthorized possession, use of, or attempting to bring a controlled substance, illegal drug or non-prescribed medication to any work site.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Information Technology Use

321.1 PURPOSE AND SCOPE

321.1.1 DEFINITIONS
Definitions related to this policy include:

Computer system - All computers (on-site and portable), electronic devices, hardware, software, and resources owned, leased, rented or licensed by the Madison County Sheriff's Office that are provided for official use by its members. This includes all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the Department or department funding.

Hardware - Includes, but is not limited to, computers, computer terminals, network equipment, electronic devices, telephones (including cellular and satellite), pagers, modems or any other tangible computer device generally understood to comprise hardware.

Software - Includes, but is not limited to, all computer programs, systems and applications, including shareware. This does not include files created by the individual user.

Temporary file, permanent file or file - Any electronic document, information or data residing or located, in whole or in part, on the system including, but not limited to, spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, messages, photographs or videos.

321.2 POLICY
It is the policy of the Madison County Sheriff's Office that members shall use information technology resources, including computers, software and systems, that are issued or maintained by the Department in a professional manner and in accordance with this policy.

321.3 PRIVACY EXPECTATION
Members forfeit any expectation of privacy with regard to emails, texts or anything published, shared, transmitted or maintained through file-sharing software or any Internet site that is accessed, transmitted, received or reviewed on any department computer system.

The Department reserves the right to access, audit and disclose, for whatever reason, any message, including attachments, and any information accessed, transmitted, received or reviewed over any technology that is issued or maintained by the Department, including the department email system, computer network and/or any information placed into storage on any department system or device. This includes records of all key strokes or Web-browsing history made at any department computer or over any department network. The fact that access to a database, service or website requires a username or password will not create an expectation of privacy if it is accessed through department computers, electronic devices or networks.

321.4 RESTRICTED USE
Members shall not access computers, devices, software or systems for which they have not received prior authorization or the required training. Members shall immediately report

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

unauthorized access or use of computers, devices, software or systems by another member to their supervisors or Shift Supervisors. Refer to the Protected Information Policy for additional guidance.

Members shall not use another person's access passwords, logon information and other individual security data, protocols and procedures unless directed to do so by a supervisor.

321.4.1 SOFTWARE

Members shall not copy or duplicate any copyrighted or licensed software except for a single copy for backup purposes, in accordance with the software company’s copyright and license agreement.

To reduce the risk of a computer virus or malicious software, members shall not install any unlicensed or unauthorized software on any department computer. Members shall not install personal copies of any software on any department computer.

When related to criminal investigations, software program files may be downloaded only with the approval of the information systems technology (IT) staff and with the authorization of the Sheriff or the authorized designee.

No member shall knowingly make, acquire or use unauthorized copies of computer software that is not licensed to the Department while on department premises, computer systems or electronic devices. Such unauthorized use of software exposes the Department and involved members to severe civil and criminal penalties.

Introduction of software by members should only occur as a part of the automated maintenance or update process of department- or County-approved or installed programs by the original manufacturer, producer or developer of the software. Any other introduction of software requires prior authorization from IT staff and a full scan for malicious attachments.

321.4.2 HARDWARE

Access to technology resources provided by or through the Department shall be strictly limited to department-related activities. Data stored on or available through department computer systems shall only be accessed by authorized members who are engaged in an active investigation or assisting in an active investigation, or who otherwise have a legitimate law enforcement or department-related purpose to access such data. Any exceptions to this policy must be approved by a supervisor.

321.4.3 INTERNET USE

Internet access provided by or through the Department shall be strictly limited to department-related activities. Internet sites containing information that is not appropriate or applicable to department use and which shall not be intentionally accessed include, but are not limited to, adult forums, pornography, gambling, chat rooms, and similar or related Internet sites. Certain exceptions may be permitted with the express approval of a supervisor as a function of a member’s assignment.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Downloaded information from the Internet shall be limited to messages, mail and data files.

321.4.4 OFF-DUTY USE

Members shall only use technology resources provided by the Department while on-duty or in conjunction with specific on-call assignments unless specifically authorized by a supervisor. This includes the use of telephones, cell phones, texting, email or any other off-the-clock work-related activities. This also applies to personally owned computers that are used to access department resources.

Refer to the Personal Communication Devices Policy for guidelines regarding off-duty use of personally owned technology.

321.5 PROTECTION OF SYSTEMS AND FILES

All members have a duty to protect the computer system and related systems and devices from physical and environmental damage and are responsible for the correct use, operation, care and maintenance of the computer system. Refer to the Protected Information Policy for additional guidance.

Members shall ensure department computers and access terminals are not viewable by persons who are not authorized users. Computers and terminals should be secured, users logged off and password protections enabled whenever the user is not present. Access passwords, logon information and other individual security data, protocols and procedures are confidential information and are not to be shared. Password length, format, structure and content shall meet the prescribed standards required by the computer system or as directed by a supervisor and shall be changed at intervals as directed by IT staff or a supervisor.

It is prohibited for a member to allow an unauthorized user to access the computer system at any time or for any reason. Members shall promptly report any unauthorized access to the computer system or suspected intrusion from outside sources (including the Internet) to a supervisor.

321.6 INSPECTION AND REVIEW

A supervisor or the authorized designee has the express authority to inspect or review the computer system, all temporary or permanent files, related electronic systems or devices, and any contents thereof, whether such inspection or review is in the ordinary course of his/her supervisory duties or based on cause.

Reasons for inspection or review may include, but are not limited to, computer system malfunctions, problems or general computer system failure, a lawsuit against the Department involving one of its members or a member's duties, an alleged or suspected violation of any department policy, a request for disclosure of data, or a need to perform or provide a service.

The IT staff may extract, download, or otherwise obtain any and all temporary or permanent files residing or located in or on the department computer system when requested by a supervisor or during the course of regular duties that require such information.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Department Use of Social Media

322.1 PURPOSE AND SCOPE

This policy provides guidelines to ensure that any use of social media on behalf of the Department is consistent with the department mission.

This policy does not address all aspects of social media use. Specifically, it does not address:

- Personal use of social media by department members (see the Speech, Expression and Social Networking Policy).
- Use of social media in personnel processes (see the Recruitment and Selection Policy).
- Use of social media as part of a criminal investigation, other than disseminating information to the public on behalf of this department (see the Investigation and Prosecution Policy).

322.1.1 DEFINITIONS

Definitions related to this policy include:

Social media - Any of a wide array of Internet-based tools and platforms that allow for the sharing of information, such as the department website or social networking services.

322.2 POLICY

The Madison County Sheriff's Office will use social media as a method of effectively informing the public about department services, issues, investigations, recruitment and other relevant events.

Department members shall ensure that the use or access of social media is done in a manner that protects the constitutional rights of all people.

322.3 AUTHORIZED USERS

Only members authorized by the Sheriff or the authorized designee may utilize social media on behalf of the Department. Authorized members shall use only department-approved equipment during the normal course of duties to post and monitor department-related social media, unless they are specifically authorized to do otherwise by their supervisors.

The Sheriff may develop specific guidelines identifying the type of content that may be posted. Any content that does not strictly conform to the guidelines should be approved by a supervisor prior to posting.

Requests to post information over department social media by members who are not authorized to post should be made through the member’s chain of command.

322.4 AUTHORIZED CONTENT

Only content that is appropriate for public release, that supports the department mission and that conforms to all department policies regarding the release of information may be posted.

Examples of appropriate content include:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) Announcements.

(b) Tips and information related to crime prevention.

(c) Investigative requests for information.

(d) Requests that ask the community to engage in projects that are relevant to the department mission.

(e) Real-time safety information that is related to in-progress crimes, geographical warnings or disaster information.

(f) Traffic information.

(g) Media releases.

(h) Recruitment of personnel.

322.4.1 INCIDENT-SPECIFIC USE

In instances of active incidents where speed, accuracy and frequent updates are paramount (e.g., crime alerts, public safety information, traffic issues), the Public Information Officer or the authorized designee will be responsible for the compilation of information to be released, subject to the approval of the Incident Commander.

322.5 PROHIBITED CONTENT

Content that is prohibited from posting includes, but is not limited to:

(a) Content that is abusive, discriminatory, inflammatory or sexually explicit.

(b) Any information that violates individual rights, including confidentiality and/or privacy rights and those provided under state, federal or local laws.

(c) Any information that could compromise an ongoing investigation.

(d) Any information that could tend to compromise or damage the mission, function, reputation or professionalism of the Madison County Sheriff's Office or its members.

(e) Any information that could compromise the safety and security of department operations, members of the Department, victims, suspects or the public.

(f) Any content posted for personal use.

(g) Any content that has not been properly authorized by this policy or a supervisor.

Any member who becomes aware of content on this department’s social media site that he/she believes is unauthorized or inappropriate should promptly report such content to a supervisor. The supervisor will ensure its removal from public view and investigate the cause of the entry.

322.5.1 PUBLIC POSTING PROHIBITED

Department social media sites shall be designed and maintained to prevent posting of content by the public.

The Department may provide a method for members of the public to contact department members directly.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

322.6 MONITORING CONTENT

The Sheriff will appoint a supervisor to review, at least annually, the use of department social media and report back on, at a minimum, the resources being used, the effectiveness of the content, any unauthorized or inappropriate content and the resolution of any issues.

322.7 RETENTION OF RECORDS

The Administration Division Supervisor should work with the Custodian of Records to establish a method of ensuring that public records generated in the process of social media use are retained in accordance with established records retention schedules.

322.8 TRAINING

Authorized members should receive training that, at a minimum, addresses legal issues concerning the appropriate use of social media sites, as well as privacy, civil rights, dissemination and retention of information posted on department sites.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Report Preparation

323.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance to those members of the Department who complete investigations and reports as a part of their duties.

323.2 POLICY

It is the policy of the Madison County Sheriff's Office that members shall act with promptness and efficiency in the preparation and processing of all reports. Reports shall document sufficient information to refresh the member’s memory and shall provide enough detail for follow-up investigation and successful prosecution.

323.3 EXPEDITIOUS REPORTING

Incomplete reports, unorganized reports or reports that are delayed without supervisory approval are not acceptable. Reports shall be processed according to established priorities or to a special priority made necessary under exceptional circumstances.

323.4 REPORT PREPARATION

Reports should be sufficiently detailed for their purpose and free from errors prior to submission and approval. It is the responsibility of the member to complete and submit all reports taken during the shift before going off-duty unless permission to hold the report has been approved by a supervisor. Generally, reports requiring prompt follow-up action on active leads or arrest reports where the suspect remains in custody should not be held.

All reports shall accurately reflect the identity of the persons involved; all pertinent information seen, heard or assimilated by any other sense; and any actions taken. Members shall not suppress, conceal or distort the facts of any reported incident, nor shall any member make a false report orally or in writing. Generally, the reporting member’s opinions should not be included in reports unless specifically identified as such.

323.4.1 HANDWRITTEN OR TYPED REPORTS

County, state and federal agency forms may be block printed unless the requirement for typing is apparent. Supervisors may require block printing or typing of reports of any nature for department consistency.

Handwritten reports must be prepared legibly. If the report is not legible, the submitting member will be required by the reviewing supervisor to promptly make corrections and resubmit the report.

In general, the narrative portion of reports where an arrest is made or when there is a long narrative should be typed or dictated. Members who dictate reports shall use appropriate grammar, as the content is not the responsibility of the typist.

Members who generate reports on computers are subject to all requirements of this policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

323.4.2 ELECTRONIC SIGNATURES

The Madison County Sheriff's Office has established an electronic signature procedure for use by all members of the Madison County Sheriff's Office. The Patrol Division Supervisor shall be responsible for maintaining the electronic signature system, ensuring that each member creates a unique, confidential password for his/her electronic signature (Va. Code § 59.1-485).

(a) Members may only use their electronic signatures for official reports or other official communications.

(b) Each member shall be responsible for the security and use of his/her electronic signature and shall promptly notify a supervisor if the electronic signature has or may have been compromised or misused.

323.5 REQUIRED REPORTING

In all of the following situations, members shall complete reports using the appropriate department-approved forms and reporting methods, unless otherwise approved by a supervisor. The reporting requirements are not intended to be all-inclusive. A member may complete a report if he/she deems it necessary or as directed by a supervisor.

323.5.1 CRIMINAL ACTIVITY

When a member responds to a call for service, or as a result of self-initiated activity becomes aware of any activity where a crime has occurred, the member shall document the incident regardless of whether a victim desires prosecution or the jurisdiction of the offense cannot be determined.

Activity to be documented in a written report includes:

(a) All arrests.

(b) All felony crimes.

(c) Non-felony criminal incidents involving threats or stalking behavior.

(d) Situations covered by separate policy. These include:

1. Use of Force Policy.
2. Domestic or Family Violence Policy.
3. Child Abuse Policy.
4. Adult Abuse Policy.
5. Hate Crimes Policy.
6. Suspicious Activity Reporting Policy.

(e) All misdemeanor crimes where the victim desires a report.

(f) Criminal and non-criminal cases initiated by law enforcement employees.

(g) When a summons is issued.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Report Preparation

Misdemeanor crimes where the victim does not desire a report shall be documented using the department-approved alternative reporting method (e.g., a dispatch log).

323.5.2 NON-CRIMINAL ACTIVITY

Non-criminal activity to be documented includes:

(a) Any found property or found evidence.

(b) All protective custody and welfare detentions.

(c) Any time a person is reported missing, regardless of jurisdiction (see the Missing Persons Policy).

(d) Suspicious incidents that may indicate a potential for crimes against children or that a child's safety is in jeopardy.

(e) Suspicious incidents that may place the public or others at risk.

(f) Any use of force by members of this department against any person (see the Use of Force Policy).

(g) Any firearm discharge (see the Firearms Policy).

(h) Any time a member points a firearm at any person.

(i) Any traffic accidents above the minimum reporting level (see the Traffic Accidents Policy).

(j) Whenever the member believes the circumstances should be documented or at the direction of a supervisor.

323.5.3 MISCELLANEOUS INJURIES

Any injury that is reported to this department shall require a report when:

(a) The injury is a result of drug overdose.

(b) There is an attempted suicide.

(c) The injury is major or serious, and potentially fatal.

(d) The circumstances surrounding the incident are suspicious in nature and it is desirable to document the event.

323.5.4 DEATHS

Death investigations require specific investigation methods, depending on the circumstances. They should be handled in accordance with the Death Investigation Policy. The handling member should notify and apprise a supervisor of the circumstances surrounding the incident to determine how to proceed. The following incidents shall be appropriately investigated and documented:

(a) Unattended deaths (no physician or qualified hospice care during the period preceding death)

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Sudden, accidental or suspicious deaths

(c) Suicides

(d) Homicide or suspected homicide

(e) Found dead bodies or body parts

323.5.5 COUNTY PERSONNEL OR PROPERTY
Incidents involving County personnel or property shall require a report when:

(a) An injury occurs as the result of an act of a County employee or on County property.

(b) There is damage to County property or equipment.

323.6 ALTERNATIVE REPORTING FOR VICTIMS

Reports that may be submitted by the public via online or other self-completed reporting processes include:

(a) Lost property.

(b) Misdemeanor thefts of property, other than firearms or materials threatening to public safety, when there is no suspect information or serial number or ability to trace the item.

1. Misdemeanor thefts of cellular telephones may be reported even though they have a serial number.

(c) Misdemeanor vandalism with no suspect information and no hate crime implications.

(d) Vehicle burglaries with no suspect information or evidence.

(e) Stolen vehicle attempts with no suspect information or evidence.

(f) Annoying telephone calls with no suspect information.

(g) Identity theft without an identifiable suspect.

(h) Online or email fraud solicitations without an identifiable suspect and if the financial loss classifies the crime as a misdemeanor.

(i) Hit-and-run vehicle accidents with no suspect or suspect vehicle.

(j) Supplemental property lists.

Members at the scene of one of the above incidents should not refer the reporting party to any alternative means of reporting without authorization from a supervisor. Members may refer victims to online victim assistance programs (e.g., the Federal Communications Commission (FCC) website for identity theft; the Internet Crime Complaint Center (IC3) website for computer crimes).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

323.7 REVIEW AND CORRECTIONS

Supervisors shall review reports for content and accuracy. If a correction is necessary, the reviewing supervisor should complete a correction form stating the reasons for rejection.

The original report and the correction form should be returned to the reporting member for correction as soon as practicable. It shall be the responsibility of the originating member to ensure that any report returned for correction is processed in a timely manner.

323.7.1 CHANGES AND ALTERATIONS

Reports that have been approved by a supervisor and submitted to the Records Division for filing and distribution shall not be modified or altered except by way of a supplemental report.

Reviewed reports that have not yet been submitted to the Records Division may be corrected or modified by the authoring member only with the knowledge and authorization of the reviewing supervisor.

323.8 NOTICE TO SCHOOLS

Anytime that a deputy arrests an adult who he/she knows or later discovers is a student in any public school division, for any of the offenses covered by Va. Code § 19.2-83.1, the Patrol Division Supervisor shall file a report with the division superintendent as soon as practicable.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Media Relations

324.1 PURPOSE AND SCOPE

This policy provides guidelines for the release of official department information to the media. It also addresses coordinating media access to scenes of disasters, criminal investigations, emergencies and other law enforcement activities.

324.2 POLICY

It is the policy of the Madison County Sheriff's Office to protect the privacy rights of individuals, while releasing non-confidential information to the media regarding topics of public concern. Information that has the potential to negatively affect ongoing investigations will not be released.

324.3 RESPONSIBILITIES

The ultimate authority and responsibility for the release of information to the media shall remain with the Sheriff. In situations not warranting immediate notice to the Sheriff and in situations where the Sheriff has given prior approval, Division Supervisors, and designated Public Information Officers (PIOs) may prepare and release information to the media, arrange and assist at scheduled news conferences and be readily available on an on-call basis to respond to the media in accordance with this policy and applicable laws regarding confidentiality.

324.4 PROVIDING ADVANCE INFORMATION

To protect the safety and rights of department members and other persons, advance information about planned actions by law enforcement personnel, such as movement of persons in custody or the execution of an arrest or search warrant, should not be disclosed to the media, nor should media representatives be invited to be present at such actions except with the prior approval of the Sheriff.

Any exceptions to the above should only be considered for the furtherance of legitimate law enforcement purposes. Prior to approving any exception, the Sheriff will consider, at a minimum, whether the release of information or the presence of the media would unreasonably endanger any individual or prejudice the rights of any person or is otherwise prohibited by law.

324.5 MEDIA REQUESTS

Any media request for information or access to a law enforcement incident shall be referred to the PIO or, if unavailable, to the first available supervisor. Prior to releasing any information to the media, members shall consider the following:

(a) At no time shall any member of this department make any comment or release any official information to the media without prior approval from a supervisor or the PIO.

(b) In situations involving multiple agencies or government departments, every reasonable effort should be made to coordinate media releases with the authorized representative of each involved agency prior to the release of any information by this department.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) Under no circumstance should any member of this department make any comment to the media regarding any law enforcement incident not involving this department without prior approval of the Sheriff. Under these circumstances the member should direct the media to the agency handling the incident.

324.6 ACCESS

Authorized media representatives shall be provided access to scenes of disasters, criminal investigations, emergencies and other law enforcement activities as required by law.

Access by the media is subject to the following conditions (Va. Code § 15.2-1714):

(a) The media representative shall produce valid media credentials that shall be prominently displayed at all times while in areas otherwise closed to the public.

(b) Media representatives should be prevented from interfering and may be removed for interfering with emergency operations and criminal investigations.

1. Based upon available resources, reasonable effort should be made to provide a safe staging area for the media that is near the incident and that will not interfere with emergency or criminal investigation operations. All information released to the media should be coordinated through the PIO or other designated spokesperson.

(c) Media interviews with individuals who are in custody should not be permitted without the approval of the Sheriff and the express written consent of the person in custody.

(d) No member of this department who is under investigation shall be subjected to media visits or interviews without the consent of the involved member.

324.6.1 CRITICAL OPERATIONS

A critical incident or tactical operation should be handled in the same manner as a crime scene, except the media should not be permitted within the inner perimeter of the incident, subject to any restrictions as determined by the supervisor in charge. Department members shall not jeopardize a critical incident or tactical operation in order to accommodate the media. All comments to the media shall be coordinated through a supervisor or the PIO.

324.6.2 TEMPORARY FLIGHT RESTRICTIONS

Whenever the presence of media or other aircraft pose a threat to public or member safety or significantly hamper incident operations, the field supervisor should consider requesting a Temporary Flight Restriction (TFR). All requests for a TFR should be routed through the Shift Supervisor. The TFR request should include specific information regarding the perimeter and altitude necessary for the incident and should be requested through the appropriate control tower. If the control tower is not known, the Federal Aviation Administration (FAA) should be contacted (14 CFR 91.137).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

324.7 CONFIDENTIAL OR RESTRICTED INFORMATION

It shall be the responsibility of the PIO to ensure that confidential or restricted information is not inappropriately released to the media (see the Records Maintenance and Release and Personnel Records policies). When in doubt, authorized and available legal counsel should be consulted prior to releasing any information.

324.7.1 EMPLOYEE INFORMATION

The identities of deputies involved in shootings or other critical incidents may only be released to the media upon the consent of the involved deputy or upon a formal request filed.

Any requests for copies of related reports or additional information not contained in the information log (see the Information Log section in this policy), including the identity of deputies involved in shootings or other critical incidents, shall be referred to the PIO.

Requests should be reviewed and fulfilled by the Custodian of Records, or if unavailable, the Shift Supervisor or the authorized designee. Such requests will be processed in accordance with the provisions of the Records Maintenance and Release Policy and public records laws (e.g., Virginia Freedom of Information Act).

324.8 RELEASE OF INFORMATION

The Department may routinely release information to the media without receiving a specific request. This may include media releases regarding critical incidents, information of public concern, updates regarding significant incidents or requests for public assistance in solving crimes or identifying suspects. This information may also be released through the department website or other electronic data sources.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Subpoenas and Court Appearances

325.1 PURPOSE AND SCOPE

This policy establishes the guidelines for department members who must appear in court. It will allow the Madison County Sheriff's Office to cover any related work absences and keep the Department informed about relevant legal matters.

325.2 POLICY

Madison County Sheriff's Office members will respond appropriately to all subpoenas and any other court-ordered appearances.

325.3 SUBPOENAS

Only department members authorized to receive a subpoena on behalf of this department or any of its members may do so.

325.3.1 SPECIAL NOTIFICATION REQUIREMENTS

Any member who is subpoenaed to testify, agrees to testify or provides information on behalf or at the request of any party other than the Commonwealth Attorney shall notify his/her immediate supervisor without delay regarding, as appropriate:

(a) Any civil case where the County or one of its members, as a result of his/her official capacity, is a party.

(b) Any civil case where any other city, county, state or federal unit of government or a member of any such unit of government, as a result of his/her official capacity, is a party.

(c) Any criminal proceeding where the member is called to testify or provide information on behalf of the defense.

(d) Any civil action stemming from the member's on-duty activity or because of his/her association with the Madison County Sheriff's Office.

(e) Any personnel or disciplinary matter when called to testify or to provide information by a government entity other than the Madison County Sheriff's Office.

The supervisor will then notify the Sheriff and the appropriate prosecuting attorney as may be indicated by the case. The Sheriff should determine if additional legal support is necessary.

No member shall be retaliated against for testifying in any matter.

325.3.2 CIVIL SUBPOENA

The Department will compensate members who appear in their official capacities on civil matters arising out of their official duties, as directed by the current County rule or policy.

The Department should seek reimbursement for the member's compensation through the civil attorney of record who subpoenaed the member.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

325.3.3 OFF-DUTY RELATED SUBPOENAS

Members receiving valid subpoenas for off-duty actions not related to their employment or appointment will not be compensated for their appearance. Arrangements for time off shall be coordinated through their immediate supervisors.

325.4 FAILURE TO APPEAR

Any member who fails to comply with the terms of any properly served subpoena or court-ordered appearance may be subject to discipline. This includes properly served orders to appear that were issued by a state administrative agency.

325.5 STANDBY

To facilitate standby agreements, members are required to provide and maintain current information on their addresses and contact telephone numbers with the Department.

If a member on standby changes his/her location during the day, the member shall notify the designated department member of how he/she can be reached. Members are required to remain on standby until released by the court or the party that issued the subpoena.

325.6 COURTROOM PROTOCOL

When appearing in court, members shall:

(a) Be punctual and prepared to proceed immediately with the case for which they are scheduled to appear.

(b) Dress in the department uniform or business attire.

(c) Observe all rules of the court in which they are appearing and remain alert to changes in the assigned courtroom where their matter is to be heard.

325.6.1 TESTIMONY

Before the date of testifying, the subpoenaed member shall request a copy of relevant reports and become familiar with the content in order to be prepared for court.

325.7 OVERTIME APPEARANCES

When a member appears in court on his/her off-duty time, he/she will be compensated in accordance with the current Madison County Sheriff's Office policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Part-Time Deputies

326.1 PURPOSE AND SCOPE

This policy establishes the guidelines for Madison County Sheriff's Office part-time deputies to supplement and assist regular full-time sheriff's deputies in their duties. These deputies provide professional and special functions and part-time services that can augment regular staffing levels.

326.1.1 DEFINITIONS

Definitions related to this policy include:

Part-time deputy- A sworn deputy with the Madison County Sheriff's Office who is employed on a regular basis and works less than a full-time position, but more than 20 hours per week, and as may be regulated by law (1 VAC 55-20-20).

326.2 POLICY

The Madison County Sheriff's Office shall ensure that part-time deputies are properly appointed, trained and supervised and that they maintain the appropriate certifications and readiness to carry out their assigned duties.

326.3 RECRUITMENT AND SELECTION

The Madison County Sheriff's Office shall endeavor to recruit and appoint only those applicants who meet the high ethical, moral and professional standards set forth by this department.

All applicants shall be required to meet and pass the same pre-employment procedures as regular full-time sheriff's deputies before appointment.

326.3.1 APPOINTMENT

Applicants who are selected for appointment as part-time deputies shall, on the recommendation of the Sheriff, be sworn in and take the Oath of Office in accordance with the Oath of Office Policy and as required for the position.

Part-time deputies are considered at-will employees and may be dismissed at the discretion of the Sheriff, with or without cause. Part-time deputies shall have no property interest in continued appointment. However, if a part-time deputy is removed for alleged misconduct, the part-time deputy will be afforded an opportunity solely to clear his/her name through a liberty interest hearing, which shall be limited to a single appearance before the Sheriff or the authorized designee.

326.4 IDENTIFICATION AND UNIFORMS

Part-time deputies will be issued Madison County Sheriff's Office uniforms, badges and identification cards. The uniforms and badges shall be the same as those worn by regular full-time sheriff's deputies. The identification cards will be the standard Madison County Sheriff's Office identification cards.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Part-Time Deputies

326.5 AUTHORITY

Part-time deputies shall perform law enforcement officer duties within the scope of their approved training (Va. Code § 9.1-101 et seq.). Part-time deputies:

(a) Perform law enforcement functions and have the authority to arrest on behalf of this department (Va. Code § 19.2-81).

(b) Shall not exercise law enforcement officer duties when off-duty.

326.6 COMPENSATION

Compensation for part-time deputies is provided as follows:

(a) Part-time deputies shall be compensated as prescribed by the ordinances of the County of Madison County, Virginia.

(b) Part-time deputies are issued two sets of uniforms and all designated attire and safety equipment, as applicable to their positions. All property issued to part-time deputies shall be returned to this department upon termination or resignation.

326.7 PERSONNEL WORKING AS PART-TIME

Qualified regular department personnel, when authorized, may also serve as part-time deputies. However, this department shall not utilize the services of part-time deputies in such a way that it would violate employment laws or labor agreements (e.g., a detention deputy working as a part-time deputy for reduced pay or no pay). Therefore, the part-time deputy coordinator should consult with the Human Resources Department prior to allowing regular department personnel to serve in a part-time deputy capacity (29 CFR 553.30).

326.8 COMPLIANCE

Part-time deputies shall be required to adhere to all department policies and procedures. A copy of the policies and procedures will be made available to each part-time deputy upon appointment. The deputies shall become thoroughly familiar with these policies.

Whenever a rule, regulation or guideline in this Policy Manual refers to a regular full-time sheriff's deputy, it shall also apply to a part-time deputy, unless by its nature it is inapplicable.

Part-time deputies are required by this department to meet department-approved training requirements.

All part-time deputies are required to attend scheduled meetings. Any absences must be satisfactorily explained to the part-time deputy coordinator.

326.9 FIREARMS

Part-time deputies shall successfully complete department-authorized training in the use of firearms. Their appointments must be approved by the County prior to being issued firearms by this department or otherwise acting as part-time deputies on behalf of the Madison County Sheriff's Office.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Part-Time Deputies

Part-time deputies will be issued duty firearms as specified in the Firearms Policy. Any part-time deputy who is permitted to carry a firearm other than the assigned duty weapon or any optional firearm may do so only in compliance with the Firearms Policy.

Part-time deputies are required to maintain proficiency with firearms used in the course of their assignments. Part-time deputies shall comply with all training and qualification requirements set forth in the Firearms Policy.

326.9.1 CONCEALED FIREARMS

An instance may arise where a part-time deputy is assigned to a plainclothes detail for his/her assigned tour of duty. Under these circumstances, the part-time deputy may be permitted to carry a weapon more suited to the assignment, but only with the knowledge and approval of the supervisor in charge of the detail.

Any part-time deputy who is permitted to carry a firearm other than the assigned duty weapon may do so only after verifying that the weapon conforms to department standards. The weapon shall comply with all the requirements set forth in the Firearms Policy.

Before being allowed to carry any optional firearm during an assigned tour of duty, the part-time deputy shall demonstrate his/her proficiency with the weapon.

326.10 PART-TIME DEPUTY COORDINATOR

The Sheriff shall delegate certain responsibilities to a part-time deputy coordinator. The coordinator shall be appointed by and directly responsible to the Patrol Division Supervisor or the authorized designee.

The part-time deputy coordinator may appoint a senior part-time member or other designee to assist in the coordination of part-time deputies and their activities.

The responsibilities of the coordinator or the authorized designee include, but are not limited to:

(a) Assigning part-time deputies.

(b) Conducting part-time deputy meetings.

(c) Establishing and maintaining a part-time deputy callout roster.

(d) Maintaining and ensuring performance evaluations are completed.

(e) Monitoring the field training progress of part-time deputies.

(f) Monitoring individual part-time deputy performance.

(g) Monitoring overall part-time deputy activities.

(h) Maintaining a liaison with other agency part-time deputy coordinators.

326.11 FIELD TRAINING

All part-time deputies shall complete the same department-specified field training as regular full-time sheriff's deputies, as described in the Field Training Policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Part-Time Deputies

326.12 SUPERVISION

Part-time deputies may perform the same duties as regular full-time deputies of this department provided they are under the direct or indirect supervision of a supervisor or deputy in charge. Part-time deputies should not supervise a regular full-time deputy.

326.12.1 EVALUATIONS

While in training, part-time deputies should be continuously evaluated using standardized daily and weekly observation reports. The part-time deputy will be considered a trainee until he/she has satisfactorily completed training. Part-time deputies who have completed their field training should be evaluated annually using performance dimensions applicable to the duties and authorities granted to that part-time deputy.

326.12.2 INVESTIGATIONS AND COMPLAINTS

If a part-time deputy has a personnel complaint made against him/her or becomes involved in an internal investigation, the matter shall be investigated in compliance with the Personnel Complaints Policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Auxiliary Positions

327.1 PURPOSE AND SCOPE

This policy establishes the guidelines for Madison County Sheriff's Office auxiliary deputies and auxiliary traffic control members to supplement and assist regular full-time sheriff's deputies in their duties. These members provide volunteer professional and special functions that augment regular staffing levels.

327.1.1 DEFINITIONS

Definitions related to this policy include:

Auxiliarydeputy - A person who is a member of the Madison County Sheriff's Office's auxiliary unit and who is authorized to exercise police powers (Va. Code § 15.2-1731).

Auxiliary traffic control member - A person deputized for the limited purpose of directing traffic (Va. Code § 46.2-1310).

327.2 POLICY

The Madison County Sheriff's Office shall ensure that auxiliary deputies are properly appointed, trained and supervised and that they maintain the appropriate certifications and readiness to carry out their assigned duties.

327.3 RECRUITMENT AND SELECTION

The Madison County Sheriff's Office shall endeavor to recruit and appoint only those applicants who meet the high ethical, moral and professional standards set forth by this department.

All applicants shall be required to meet and pass the same pre-employment procedures as regular sheriff's deputies before appointment.

327.3.1 APPOINTMENT

Applicants who are selected for appointment as auxiliary deputies shall, on the recommendation of the Sheriff, be sworn in and take the Oath of Office in accordance with the Oath of Office Policy and as required for the position.

Auxiliary deputies are considered at-will employees and may be dismissed at the discretion of the Sheriff, with or without cause. Auxiliary deputies shall have no property interest in continued appointment. However, if an auxiliary deputy is removed for alleged misconduct, the auxiliary deputy will be afforded an opportunity solely to clear his/her name through a liberty interest hearing, which shall be limited to a single appearance before the Sheriff or the authorized designee (Va. Code § 15.2-1733).

327.4 IDENTIFICATION AND UNIFORMS

Auxiliary deputies will be issued Madison County Sheriff's Office uniforms, badges and identification cards. The uniforms and badges shall be the same as those worn by regular full-time

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

sheriff's deputies. The identification cards will be the standard Madison County Sheriff's Office identification cards.

327.5 AUTHORITY

Auxiliary deputies shall perform law enforcement officer duties within the scope of their approved training (Va. Code § 15.2-1731). Auxiliary deputies:

(a) Perform law enforcement functions and have the authority to arrest on behalf of this department (Va. Code § 15.2-1731).

(b) Shall not exercise law enforcement officer duties when off-duty.

327.6 COMPENSATION

Compensation for auxiliary deputies is provided as follows (Va. Code § 15.2-1731):

(a) Auxiliary deputies shall be compensated as prescribed by the ordinances of the County of Madison County, Virginia.

(b) Auxiliary deputies shall be issued a uniform and all designated attire and safety equipment, as applicable to their positions. All property issued to auxiliary deputies shall be returned to this department upon termination or resignation.

(c) Auxiliary deputies are not eligible to participate in any pension program provided for regular deputies.

327.7 PERSONNEL WORKING AS AUXILIARY DEPUTIES

Qualified regular department personnel, when authorized, may also serve as auxiliary deputies. However, this department shall not utilize the services of auxiliary deputies in such a way that it would violate employment laws or labor agreements (e.g., a detention deputy working as an auxiliary deputy for reduced or no pay). Therefore, the auxiliary coordinator should consult with the Human Resources Department prior to allowing regular department personnel to serve in an auxiliary deputy capacity (29 CFR 553.30).

327.8 COMPLIANCE

Auxiliary deputies shall be required to adhere to all department policies and procedures. A copy of the policies and procedures will be made available to each auxiliary deputy upon appointment. The auxiliary deputy shall become thoroughly familiar with these policies.

Whenever a rule, regulation, or guideline in this Policy Manual refers to a regular full-time sheriff's deputy, it shall also apply to an auxiliary deputy, unless by its nature it is inapplicable.

Auxiliary deputies are required by this department to meet department-approved training requirements and all requirements of the Administrative Code of Virginia prior to performing authorized duties.

All auxiliary deputies are required to attend scheduled meetings and meet all training requirements of the Department and the Administrative Code of Virginia. Any absences must be satisfactorily explained to the auxiliary coordinator.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

327.9 FIREARMS

Auxiliary deputies shall successfully complete department-authorized training in the use of firearms. Their appointments must be approved by the County prior to being issued firearms by this department or otherwise acting as auxiliary deputies on behalf of the Madison County Sheriff's Office.

Auxiliary deputies will be issued duty firearms as specified in the Firearms Policy. Any auxiliary deputy who is permitted to carry a firearm other than the assigned duty weapon or any optional firearm may do so only in compliance with the Firearms Policy.

Auxiliary deputies are required to maintain proficiency with firearms used in the course of their assignments. Auxiliary deputies shall comply with all training and qualification requirements set forth in the Firearms Policy.

327.9.1 CONCEALED FIREARMS

An auxiliary deputy shall not carry a concealed firearm while in an off-duty capacity, other than to and from work, unless he/she possesses a valid concealed handgun permit.

An instance may arise where an auxiliary deputy is assigned to a plainclothes detail for his/her assigned tour of duty. Under these circumstances, the auxiliary deputy may be permitted to carry a weapon more suited to the assignment, but only with the knowledge and approval of the supervisor in charge of the detail.

Any auxiliary deputy who is permitted to carry a firearm other than the assigned duty weapon may do so only after verifying that the weapon conforms to department standards. The weapon shall comply with all the requirements set forth in the Firearms Policy.

Before being allowed to carry any optional firearm during an assigned tour of duty, the auxiliary deputy shall demonstrate his/her proficiency with the weapon.

327.10 AUXILIARY COORDINATOR

The Sheriff shall delegate certain responsibilities to an auxiliary coordinator. The auxiliary coordinator shall be appointed by and directly responsible to the Patrol Division Supervisor or the authorized designee.

The auxiliary coordinator may appoint a senior auxiliary deputy or other designee to assist in the coordination of auxiliary deputies and their activities.

The responsibilities of the coordinator or the authorized designee include, but are not limited to:

(a) Assigning auxiliary deputies.

(b) Conducting auxiliary deputy meetings.

(c) Establishing and maintaining an auxiliary deputy callout roster.

(d) Maintaining and ensuring performance evaluations are completed.

(e) Monitoring the field training progress of auxiliary deputies.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(f) Monitoring individual auxiliary deputy performance.

(g) Monitoring overall auxiliary deputy activities.

(h) Maintaining a liaison with other agency auxiliary coordinators.

327.11 FIELD TRAINING

All auxiliary deputies shall complete the same department-specified field training as regular full-time sheriff's deputies as described in the Field Training Policy.

327.12 SUPERVISION

Auxiliary deputies may perform the same duties as regular full-time deputies of this department provided they are under the direct or indirect supervision of a supervisor or deputy in charge. Auxiliary deputies shall never supervise a regular full-time deputy.

327.12.1 EVALUATIONS

While in training, auxiliary deputies should be continuously evaluated using standardized daily and weekly observation reports. The auxiliary deputy will be considered a trainee until he/she has satisfactorily completed training. Auxiliary deputies who have completed their field training should be evaluated annually using performance dimensions applicable to the duties and authorities granted to that auxiliary deputy.

327.12.2 INVESTIGATIONS AND COMPLAINTS

If an auxiliary deputy has a personnel complaint made against him/her or becomes involved in an internal investigation, the matter shall be investigated in compliance with the Personnel Complaints Policy.

327.13 AUXILIARY TRAFFIC CONTROL MEMBERS

Auxiliary traffic control members shall be deputized by the Sheriff for the limited purpose of directing traffic in accordance with Va. Code § 46.2-1309. Auxiliary traffic control members (Va. Code § 46.2-1310):

(a) Shall first receive appropriate training as necessary to perform traffic control.

(b) Do not have arrest powers.

(c) Shall wear a distinctive uniform, safety vest or a white reflective belt which crosses both the chest and back above the waist.

(d) May be assigned at the discretion of the Sheriff, Division Supervisors and Shift Supervisor during periods of heavy traffic or congestion.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Outside Agency Assistance

328.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance to members when requesting or responding to a request for mutual aid or when assisting another law enforcement agency.

328.2 POLICY

It is the policy of the Madison County Sheriff's Office to promptly respond to requests for assistance by other law enforcement agencies, subject to available resources and consistent with the applicable laws and policies of this department.

328.3 ASSISTING OUTSIDE AGENCIES

Generally, requests for any type of assistance from another agency should be routed to the Shift Supervisor's office for approval. In some instances, a county rule or policy or other established agreement or protocol may exist that eliminates the need for approval of individual requests.

When another law enforcement agency requests assistance from this department, the Shift Supervisor may authorize, if available, an appropriate number of personnel to assist. Members are reminded that their actions when rendering assistance must conform with applicable laws and be consistent with the policies of this department.

Deputies may respond to a request for emergency assistance; however, they shall notify a supervisor of their activity as soon as practicable.

Arrestees may be temporarily detained by this department until arrangements for transportation are made by the outside agency. Probation violators who are temporarily detained by this department will not ordinarily be booked at this department. Only in exceptional circumstances, and subject to supervisor approval, will this department provide transportation of arrestees to other facilities on behalf of another agency.

When transportation assistance is rendered, a report shall be prepared and submitted by the handling member unless otherwise directed by a supervisor.

328.3.1 INITIATED ACTIVITY

Any on-duty deputy who engages in law enforcement activities of any type that are not part of a mutual aid request and take place outside the jurisdiction of the Madison County Sheriff's Office is acting as a private citizen and without law enforcement powers. They are, however, on-duty and shall notify their supervisor or the Shift Supervisor and the Dispatch Center as soon as practicable. This requirement does not apply to special enforcement details or multi-agency units that regularly work in multiple jurisdictions.

328.3.2 CONTRACT SERVICES

The Madison County Sheriff's Office may also provide contracted law enforcement services at the direction of the Sheriff, as authorized by resolution of the County legislative authority. The contract for law enforcement services shall contain:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) A detailed description of the specific services to be provided

(b) The financial terms of the contract

(c) A statement of the records to be maintained by the department

(d) The duration of the contract

(e) The process by which the contract may be modified or terminated

(f) Insurance and liability coverage

(g) A stipulation that supervision and control of members will remain with the Madison County Sheriff's Office

(h) Arrangements for the use of department equipment and facilities

328.4 REQUESTING OUTSIDE ASSISTANCE

If assistance is needed from another agency, the member requesting assistance should, if practicable, first notify a supervisor. The handling member or supervisor should direct assisting personnel to where they are needed and to whom they should report when they arrive.

The requesting member should arrange for appropriate radio communication capabilities, if necessary and available, so that communication can be coordinated between assisting personnel.

328.5 REPORTING REQUIREMENTS

Incidents of outside assistance or law enforcement activities that are not documented in a crime report shall be documented in a general case report or as directed by the Shift Supervisor.

328.6 MANDATORY SHARING

Equipment and supplies purchased with federal funds or grants that require such equipment and supplies to be shared with other agencies should be documented and updated as necessary by the Administration Division Supervisor or the authorized designee.

The documentation should include:

(a) The conditions relative to sharing.

(b) The training requirements for:

1. The use of the equipment and supplies.
2. The members trained in the use of the equipment and supplies.

(c) Any other requirements for use of the equipment and supplies.

The Training Supervisor should maintain documentation that the appropriate members have received the required training.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Registered Offender Information

329.1 PURPOSE AND SCOPE

This policy establishes guidelines by which the Madison County Sheriff's Office will address issues associated with certain offenders who are residing in the jurisdiction, and how the Department will disseminate information and respond to public inquiries for information about registered sex offenders.

329.2 POLICY

It is the policy of the Madison County Sheriff's Office to coordinate with the Virginia State Police (VSP) to identify and monitor registered offenders living within this jurisdiction and to take reasonable steps to address the risks those persons may pose.

329.3 REGISTRATION

The Major shall establish a process to reasonably accommodate registration of offenders. The process should rebut any allegation on the part of the offender that the registration process was too confusing, burdensome, or difficult for compliance. If it is reasonable to do so, an investigator assigned to related investigations should conduct the registration in order to best evaluate any threat the person may pose to the community. Those assigned to register offenders should receive appropriate training regarding the registration process.

Upon conclusion of the registration process, the investigator shall ensure that the registration information is provided to the Virginia State Police in accordance with Va. Code § 9.1-903 and 19 VAC 30-170-15.

The refusal of a registrant to provide any of the required information or complete the process should initiate a criminal investigation for failure to register.

329.4 MONITORING OF REGISTERED OFFENDERS

The Major should establish a system to periodically, and at least once annually, verify that a registrant remains in compliance with his/her registration requirements after the initial registration. This verification should include:

(a) Efforts to confirm residence using an unobtrusive method, such as an Internet search or drive-by of the declared residence.

(b) Review of information on the VSP Sex Offender Registry.

(c) Contact with a registrant's parole or probation officer.

Any discrepancies should be reported to the VSP.

The Sheriff should also establish a procedure to routinely disseminate information regarding registered offenders to Madison County Sheriff's Office members, including timely updates regarding new or relocated registrants.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Registered Offender Information

329.5 DISSEMINATION OF PUBLIC INFORMATION

Members will not unilaterally make a public notification advising the community of a particular registrant's presence in the community. Members who identify a significant risk or other public safety issue associated with a registrant should promptly advise their supervisor. The supervisor should evaluate the request and forward the information to the Sheriff if warranted. A determination will be made by the Sheriff, with the assistance of legal counsel as necessary, whether such a public alert should be made.

Members of the public requesting information on registrants should be directed to the VSP Sex Offender Registry or the Madison County Sheriff's Office's website.

The Sheriff or designee shall release local registered offender information to residents in accordance with Va. Code § 2.2-3704 et seq. and in compliance with a Virginia Freedom of Information Act request.

329.5.1 REGISTRY INFORMATION

A request for information specific to the VSP Sex Offender Registry may be received by this department and forwarded to the VSP (Va. Code § 9.1-912).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Major Incident Notification

330.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance to members of the Madison County Sheriff's Office in determining when, how and to whom notification of major incidents should be made.

330.2 POLICY

The Madison County Sheriff's Office recognizes that certain incidents should be brought to the attention of supervisors or other specified personnel of this department to facilitate the coordination of activities and ensure that inquiries from the media and the public may be properly addressed.

330.3 CRITERIA FOR NOTIFICATION

Most situations where the media show a strong interest are also of interest to the Sheriff, the affected Division Supervisor and the County. The following list of incident types is provided as a guide for notification and is not intended to be all inclusive:

- Officer-involved shooting, whether on- or off-duty (see the Officer-Involved Shootings and Deaths Policy for special notification)
- Homicides, suspicious deaths or deaths related to law enforcement activity
- Crimes of unusual violence or circumstances that may include hostages, barricaded persons, home invasions, armed robbery or sexual assaults
- At-risk missing children, critically missing adults or missing senior adults
- In-custody deaths
- Aircraft, train, boat or other transportation accidents with major damage and/or injury or death
- Traffic accidents with fatalities or severe injuries
- Death of a prominent Madison County, Virginia official
- Significant injury or death to a member of the Department, whether on- or off-duty
- Arrest of a member of the Department or prominent Madison County, Virginia official
- Equipment failures, utility failures and incidents that may affect staffing or pose a threat to basic sheriff's services
- Prisoner escape
- Any other incident that has attracted or is likely to attract significant media attention

330.4 SHIFT SUPERVISOR RESPONSIBILITIES

The Shift Supervisor is responsible for making the appropriate notifications. The Shift Supervisor shall make reasonable attempts to obtain as much information on the incident as possible before

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

notification, and shall attempt to make the notifications as soon as practicable. Notification should be made by using the call notification protocol posted in the Dispatch Center.

330.4.1 COMMAND STAFF NOTIFICATION

In the event an incident occurs as identified in the Criteria for Notification section above, the Sheriff shall be notified along with the affected Division Supervisor and the Investigation Division Supervisor if that division is affected.

330.4.2 INVESTIGATOR NOTIFICATION

If the incident requires that an investigator respond from home, the immediate supervisor of the appropriate detail shall be notified, who will then contact the appropriate investigator.

330.4.3 PATROL DIVISION NOTIFICATION

In the event of a major injury or traffic fatality, the Patrol Division supervisor shall be notified, who will then contact the appropriate investigator. The Patrol Division supervisor will notify the Patrol Commander.

330.4.4 PUBLIC INFORMATION OFFICER

After members of the command staff have been notified, the Public Information Officer shall be called if it appears the media may have a significant interest in the incident.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Death Investigation

331.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for situations where deputies initially respond to and investigate the circumstances of a deceased person.

Some causes of death may not be readily apparent and some cases differ substantially from what they appear to be initially. The thoroughness of death investigations and use of appropriate resources and evidence gathering techniques is critical.

331.2 POLICY

It is the policy of the Madison County Sheriff's Office to respond to, document and investigate incidents where a person is deceased. Investigations involving the death of a person, including those from natural causes, accidents, workplace incidents, suicide and homicide, shall be initiated, conducted and properly documented.

331.3 INVESTIGATION CONSIDERATIONS

Emergency medical services shall be called in all suspected death cases unless death is obvious (e.g., decapitated, decomposed).

A supervisor shall be notified as soon as possible to assist and provide appropriate personnel and resources. The on-scene supervisor should determine whether follow-up investigation is required and notify the Investigation Division Commander as necessary. The Shift Supervisor will make notification to command staff in accordance with the Major Incident Notification Policy.

331.3.1 REPORTING

All incidents involving a death shall be documented on the appropriate form.

See attachment: Death Scene Checklist.pdf

331.3.2 MEDICAL EXAMINER REQUEST

Deputies are not authorized to pronounce death unless they are also Medical Examiners, Deputy Medical Examiners or appointed Medical Examiner investigators. The Medical Examiner shall be called in all sudden or unexpected deaths or deaths due to other than natural causes. State law requires that the Medical Examiner be notified when any person dies (Va. Code § 32.1-283):

(a) As a result trauma, injury, violence, poisoning, accident, suicide or homicide.

(b) Suddenly when in apparent good health.

(c) While unattended by a physician.

(d) While in jail, prison, other correctional institution or in police custody.

(e) While receiving services in a state hospital or training center operated by the Department of Behavioral Health and Developmental Services.

(f) Suddenly as an apparent result of fire.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(g) In any suspicious, unusual or unnatural manner.

(h) Due to sudden infant death syndrome.

331.3.3 SEARCHING DEAD BODIES

(a) The Medical Examiner, his/her assistant, and authorized investigators are generally the only persons permitted to move, handle or search a dead body.

(b) When necessary, a deputy may make a reasonable search of an individual who it is reasonable to believe is dead, or near death, for the purpose of identification.

(c) The Medical Examiner, with the permission of the Department, may take property, objects, or articles found on the deceased or in the immediate vicinity of the deceased that may be necessary for conducting an investigation to determine the identity of the deceased or the cause or manner of death.

(d) Should exigent circumstances indicate to a deputy that any other search of a known dead body is warranted prior to the arrival of the Medical Examiner or his/her assistant, the investigating deputy should first obtain verbal consent from the Medical Examiner or his/her assistant when practicable.

(e) Whenever reasonably possible, a witness, preferably a relative to the deceased or a member of the household, should be requested to remain nearby the scene and available to the deputy pending the arrival of the Medical Examiner or his/her assistant. The name and address of this person shall be included in the narrative of the death report.

(f) Whenever personal effects are removed from the body of the deceased by the Medical Examiner or his/her assistant, a receipt shall be obtained. This receipt shall be attached to the death report.

331.3.4 SUSPECTED HOMICIDE

If the initially assigned deputy suspects that the death involves a homicide or other suspicious circumstances, the deputy shall take steps to protect the scene. The Investigation Division shall be notified to determine the possible need for an investigator to respond to the scene.

If the on-scene supervisor, through consultation with the Shift Supervisor or Investigation Division supervisor, is unable to determine the manner of death, the investigation shall proceed as though it is a homicide.

The investigator assigned to investigate a homicide or death that occurred under suspicious circumstances may, with the approval of his/her supervisor, request the Medical Examiner to conduct physical examinations and tests, and to provide a report.

331.3.5 EMPLOYMENT-RELATED DEATHS OR INJURIES

Any member of this department who responds to and determines that a death, serious illness or serious injury has occurred as a result of an accident at or in connection with the victim's employment should ensure that the Virginia Occupational Safety and Health (VOSH) Program and, if applicable, the regional Occupational Safety and Health Administration (OSHA) offices are

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

notified of all pertinent information. In addition any fatality or the in-patient hospitalization of three or more person as prescribed by the rules and regulations of the Virginia Safety and Health Codes Board, shall be reported within eight hours to the Virginia Department of Labor and Industry (Va. Code § 40.1-51.1).

331.4 UNIDENTIFIED DEAD BODY

If the identity of a dead body cannot be established, the handling deputy will request from the Medical Examiner a unique identifying number for the body. The number shall be included in any report.

331.5 DEATH NOTIFICATION

When reasonably practicable, and if not handled by the Medical Examiner’s Office, notification to the next-of-kin of the deceased person shall be made, in person, by the deputy assigned to the incident. If the next-of-kin lives in another jurisdiction, a law enforcement official from that jurisdiction shall be requested to make the personal notification (Va. Code § 32.1-309.1).

If a deceased person has been identified as a missing person, this department shall attempt to locate family members and inform them of the death and location of the deceased missing person's remains. All efforts to locate and notify family members shall be recorded in appropriate reports.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Private Person’s Arrest

332.1 PURPOSE AND SCOPE

This policy provides guidance for the handling and acceptance of a private person’s arrest.

332.2 POLICY

It is the policy of the Madison County Sheriff's Office to accept a private person’s arrest only when legal and appropriate.

332.3 ARRESTS BY PRIVATE PERSON

A private person may arrest another under the following circumstances:

(a) Without a warrant when the person arrested has committed a breach of the peace in his/her presence.

(b) Without a warrant when a felony has actually been committed and there is reasonable grounds for believing the person arrested has committed the crime.

(c) Without a warrant upon reasonable information that the accused stands charged in the courts of a state with a crime punishable by imprisonment for a term exceeding one year (Va. Code § 19.2-100).

332.4 DEPUTY RESPONSIBILITIES

A deputy confronted with a person claiming to have made a private person’s arrest should determine whether such an arrest is lawful.

If the deputy determines that the private person’s arrest is unlawful, the deputy should:

(a) Take no action to further detain or restrain the arrested individual, unless there is independent justification for continuing a detention.

(b) Advise the parties that the arrest will not be accepted but the circumstances will be documented in a report.

(c) Document the incident, including the basis for refusing to accept custody of the individual.

Whenever a deputy determines that a private person’s arrest is justified, the deputy may take the individual into custody and proceed in the same manner as with any other arrest.

332.5 PRIVATE PERSON’S ARREST

The arresting person should be asked to complete and sign a criminal complaint. If the person fails or refuses to do so, the arrested individual should be released, unless the deputy has a lawful reason, independent of the private person's arrest, to take the individual into custody and determines an arrest is appropriate.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Limited English Proficiency Services

333.1 PURPOSE AND SCOPE

This policy provides guidance to members when communicating with individuals with limited English proficiency (LEP) (42 USC § 2000d).

333.1.1 DEFINITIONS

Definitions related to this policy include:

Authorized interpreter - A person who has been screened and authorized by the Department to act as an interpreter and/or translator for others.

Interpret or interpretation - The act of listening to a communication in one language (source language) and orally converting it to another language (target language), while retaining the same meaning.

Limited English proficiency (LEP) individual - Any individual whose primary language is not English and who has a limited ability to read, write, speak or understand English. These individuals may be competent in certain types of communication (e.g., speaking or understanding) but still exhibit LEP for other purposes (e.g., reading or writing). Similarly, LEP designations are context-specific; an individual may possess sufficient English language skills to function in one setting but these skills may be insufficient in other situations.

Qualified bilingual member - A member of the Madison County Sheriff's Office, designated by the Department, who has the ability to communicate fluently, directly and accurately in both English and another language. Bilingual members may be fluent enough to communicate in a non-English language but may not be sufficiently fluent to interpret or translate from one language into another.

Translate or translation - The replacement of written text from one language (source language) into an equivalent written text (target language).

333.2 POLICY

It is the policy of the Madison County Sheriff's Office to reasonably ensure that LEP individuals have meaningful access to law enforcement services, programs and activities, while not imposing undue burdens on its members.

The Department will not discriminate against or deny any individual access to services, rights or programs based upon national origin or any other protected interest or right.

333.3 LEP COORDINATOR

The Sheriff shall delegate certain responsibilities to an LEP coordinator. The coordinator shall be appointed by, and directly responsible to, the Patrol Division Supervisor or the authorized designee.

The responsibilities of the coordinator include, but are not limited to:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) Coordinating and implementing all aspects of the Madison County Sheriff's Office's LEP services to LEP individuals.

(b) Developing procedures that will enable members to access LEP services, including telephonic interpreters, and ensuring the procedures are available to all members.

(c) Ensuring that a list of all qualified bilingual members and authorized interpreters is maintained and available to each Shift Supervisor and Dispatch Supervisor. The list should include information regarding:

1. Languages spoken.
2. Contact information.
3. Availability.

(d) Ensuring signage stating that interpreters are available free of charge to LEP individuals is posted in appropriate areas and in the most commonly spoken languages.

(e) Reviewing existing and newly developed documents to determine which are vital documents and should be translated, and into which languages the documents should be translated.

(f) Annually assessing demographic data and other resources, including contracted language services utilization data and data from community-based organizations, to determine if there are additional documents or languages that are appropriate for translation.

(g) Identifying standards and assessments to be used by this department to qualify individuals as qualified bilingual members or authorized interpreters.

(h) Periodically reviewing efforts of this department in providing meaningful access to LEP individuals, and, as appropriate, developing reports, developing new procedures or recommending modifications to this policy.

(i) Receiving and responding to complaints regarding department LEP services.

(j) Ensuring appropriate processes are in place to provide for the prompt and equitable resolution of complaints and inquiries regarding discrimination in access to department services, programs and activities.

333.4 FOUR-FACTOR ANALYSIS

Because there are many different languages that members could encounter, the Department will utilize the four-factor analysis outlined in the U.S. Department of Justice (DOJ) Guidance to Federal Financial Assistance Recipients, available at the DOJ website, to determine which measures will provide meaningful access to its services and programs. It is recognized that law enforcement contacts and circumstances will vary considerably. This analysis, therefore, must remain flexible and will require an ongoing balance of the following four factors, which are:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) The number or proportion of LEP individuals eligible to be served or likely to be encountered by department members, or who may benefit from programs or services within the jurisdiction of this department or a particular geographic area.

(b) The frequency with which LEP individuals are likely to come in contact with department members, programs or services.

(c) The nature and importance of the contact, program, information or service provided.

(d) The cost of providing LEP assistance and the resources available.

333.5 TYPES OF LEP ASSISTANCE AVAILABLE

Madison County Sheriff's Office members should never refuse service to an LEP individual who is requesting assistance, nor should they require an LEP individual to furnish an interpreter as a condition for receiving assistance. The Department will make every reasonable effort to provide meaningful and timely assistance to LEP individuals through a variety of services.

The Department will utilize all reasonably available tools, such as language identification cards, when attempting to determine an LEP individual's primary language.

LEP individuals may choose to accept department-provided LEP services at no cost or they may choose to provide their own.

Department-provided LEP services may include, but are not limited to, the assistance methods described in this policy.

333.6 WRITTEN FORMS AND GUIDELINES

Vital documents or those that are frequently used should be translated into languages most likely to be encountered. The LEP coordinator will arrange to make these translated documents available to members and other appropriate individuals, as necessary.

333.7 AUDIO RECORDINGS

The Department may develop audio recordings of important or frequently requested information in a language most likely to be understood by those LEP individuals who are representative of the community being served.

333.8 QUALIFIED BILINGUAL MEMBERS

Bilingual members may be qualified to provide LEP services when they have demonstrated through established department procedures a sufficient level of skill and competence to fluently communicate in both English and a non-English language. Members utilized for LEP services must demonstrate knowledge of the functions of an interpreter/translator and the ethical issues involved when acting as a language conduit. Additionally, bilingual members must be able to communicate technical and law enforcement terminology, and be sufficiently proficient in the non-English language to perform complicated tasks, such as conducting interrogations, taking statements, collecting evidence or conveying rights or responsibilities.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

When a qualified bilingual member from this department is not available, personnel from other County departments who have been identified by the Department as having the requisite skills and competence may be requested.

333.9 AUTHORIZED INTERPRETERS

Any person designated by the Department to act as an authorized interpreter and/or translator must have demonstrated competence in both English and the involved non-English language, must have an understanding of the functions of an interpreter that allows for correct and effective translation, and should not be a person with an interest in the department case or investigation involving the LEP individual. A person providing interpretation or translation services may be required to establish the accuracy and trustworthiness of the interpretation or translation in a court proceeding.

Authorized interpreters must pass a screening process established by the LEP coordinator that demonstrates their skills and abilities in the following areas:

(a) The competence and ability to communicate information accurately in both English and in the target language.

(b) Knowledge, in both languages, of any specialized terms or concepts peculiar to this department and of any particularized vocabulary or phraseology used by the LEP individual.

(c) The ability to understand and adhere to the interpreter role without deviating into other roles, such as counselor or legal adviser.

(d) Knowledge of the ethical issues involved when acting as a language conduit.

333.9.1 SOURCES OF AUTHORIZED INTERPRETERS

The Department may contract with authorized interpreters who are available over the telephone. Members may use these services with the approval of a supervisor and in compliance with established procedures.

Other sources may include:

- Qualified bilingual members of this department or personnel from other County departments.
- Individuals employed exclusively to perform interpretation services.
- Contracted in-person interpreters, such as state or federal court interpreters, among others.
- Interpreters from other agencies who have been qualified as interpreters by this department, and with whom the Department has a resource-sharing or other arrangement that they will interpret according to department guidelines.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

333.9.2 COMMUNITY VOLUNTEERS AND OTHER SOURCES OF LANGUAGE ASSISTANCE

Language assistance may be available from community volunteers who have demonstrated competence in either monolingual (direct) communication and/or in interpretation or translation (as noted in above), and have been approved by the Department to communicate with LEP individuals.

Where qualified bilingual members or other authorized interpreters are unavailable to assist, approved community volunteers who have demonstrated competence may be called upon when appropriate. However, department members must carefully consider the nature of the contact and the relationship between the LEP individual and the volunteer to ensure that the volunteer can provide neutral and unbiased assistance.

While family or friends of an LEP individual may offer to assist with communication or interpretation, members should carefully consider the circumstances before relying on such individuals. For example, children should not be relied upon except in exigent or very informal and non-confrontational situations.

333.10 CONTACT AND REPORTING

Although all law enforcement contacts, services and individual rights are important, this department will utilize the four-factor analysis to prioritize service to LEP individuals so that such services may be targeted where they are most needed, according to the nature and importance of the particular law enforcement activity involved.

Whenever any member of this department is required to complete a report or other documentation that involves a situation in which interpretation services were provided to any involved LEP individual, such services should be noted in the related report. Members should document the type of interpretation services utilized and whether the individual elected to use services provided by the Department or some other identified source.

333.11 RECEIVING AND RESPONDING TO REQUESTS FOR ASSISTANCE

The Madison County Sheriff's Office will take reasonable steps and will work with the Human Resources Department to develop in-house language capacity by hiring or appointing qualified members proficient in languages representative of the community being served.

333.11.1 EMERGENCY CALLS TO 9-1-1

Department members will make every reasonable effort to promptly accommodate LEP individuals utilizing 9-1-1 lines. When a 9-1-1 call-taker receives a call and determines that the caller is an LEP individual, the call-taker shall quickly determine whether sufficient information can be obtained to initiate an appropriate emergency response. If language assistance is still needed, the language is known and a qualified bilingual member is available in the Dispatch Center, the call shall immediately be handled by the qualified bilingual member.

If a qualified bilingual member is not available or the call-taker is unable to identify the caller’s language, the call-taker will contact the contracted telephone interpretation service and establish a three-way call between the call-taker, the LEP individual and the interpreter.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Dispatchers will make every reasonable effort to dispatch a qualified bilingual member to the assignment, if available and appropriate.

Although 9-1-1 calls shall receive top priority, reasonable efforts should also be made to accommodate LEP individuals seeking routine access to services and information by utilizing the resources listed in this policy.

333.12 FIELD ENFORCEMENT

Field enforcement will generally include such contacts as traffic stops, pedestrian stops, serving warrants and restraining orders, crowd/traffic control and other routine field contacts that may involve LEP individuals. The scope and nature of these activities and contacts will inevitably vary. Members and/or supervisors must assess each situation to determine the need and availability of language assistance to all involved LEP individuals and utilize the methods outlined in this policy to provide such assistance.

Although not every situation can be addressed in this policy, it is important that members are able to effectively communicate the reason for a contact, the need for information and the meaning or consequences of any enforcement action. For example, it would be meaningless to request consent to search if the deputy is unable to effectively communicate with an LEP individual.

If available, deputies should obtain the assistance of a qualified bilingual member or an authorized interpreter before placing an LEP individual under arrest.

333.13 INVESTIGATIVE FIELD INTERVIEWS

In any situation where an interview may reveal information that could be used as the basis for arrest or prosecution of an LEP individual and a qualified bilingual member is unavailable or lacks the skills to directly communicate with the LEP individual, an authorized interpreter should be used. This includes interviews conducted during an investigation with victims, witnesses and suspects. In such situations, audio recordings of the interviews should be made when reasonably possible. Identification and contact information for the interpreter (e.g., name, address) should be documented so that the person can be subpoenaed for trial if necessary.

If an authorized interpreter is needed, deputies should consider calling for an authorized interpreter in the following order:

- An authorized department member or allied agency interpreter
- An authorized telephone interpreter
- Any other authorized interpreter

Any *Miranda* warnings shall be provided to suspects in their primary language by an authorized interpreter or, if the suspect is literate, by providing a translated *Miranda* warning card.

The use of an LEP individual’s bilingual friends, family members, children, neighbors or bystanders may be used only when a qualified bilingual member or authorized interpreter is unavailable and there is an immediate need to interview an LEP individual.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

333.14 CUSTODIAL INTERROGATIONS

Miscommunication during custodial interrogations may have a substantial impact on the evidence presented in a criminal prosecution. Only qualified bilingual members or, if none is available or appropriate, authorized interpreters shall be used during custodial interrogations. *Miranda* warnings shall be provided to suspects in their primary language by the qualified bilingual member or an authorized interpreter.

To ensure that translations during custodial interrogations are accurately documented and are admissible as evidence, interrogations should be recorded as required by law. See guidance on recording custodial interrogations in the Investigation and Prosecution Policy.

333.15 BOOKINGS

When gathering information during the booking process, members should remain alert to the impediments that language barriers can create. In the interest of the arrestee's health and welfare, to protect the safety and security of the facility, and to protect individual rights, it is important that accurate medical screening and booking information be obtained. Members should seek the assistance of a qualified bilingual member whenever there is concern that accurate information cannot be obtained or that booking instructions may not be properly understood by an LEP individual.

333.16 COMPLAINTS

The Department shall ensure that LEP individuals who wish to file a complaint regarding members of this department are able to do so. The Department may provide an authorized interpreter or translated forms, as appropriate. Complaints will be referred to the LEP coordinator.

Investigations into such complaints shall be handled in accordance with the Personnel Complaints Policy. Authorized interpreters used for any interview with an LEP individual during a complaint investigation should not be members of this department.

Any notice required to be sent to an LEP individual as a complaining party pursuant to the Personnel Complaints Policy should be translated or otherwise communicated in a language-accessible manner.

333.17 COMMUNITY OUTREACH

Community outreach programs and other such services offered by this department are important to the ultimate success of more traditional law enforcement duties. This department will continue to work with community groups, local businesses and neighborhoods to provide equal access to such programs and services.

333.18 TRAINING

To ensure that all members who may have contact with LEP individuals are properly trained, the Department will provide periodic training on this policy and related procedures, including how to access department-authorized telephonic and in-person interpreters and other available resources.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

The Training Supervisor shall be responsible for ensuring new members receive LEP training. Those who may have contact with LEP individuals should receive refresher training at least once every two years thereafter. The Training Supervisor shall maintain records of all LEP training provided, and will retain a copy in each member's training file in accordance with the established records retention schedule.

333.18.1 TRAINING FOR AUTHORIZED INTERPRETERS

All members on the authorized interpreter list must successfully complete prescribed interpreter training. To complete interpreter training successfully, an interpreter must demonstrate proficiency in and ability to communicate information accurately in both English and in the target language, demonstrate knowledge in both languages of any specialized terms or phraseology, and understand and adhere to the interpreter role without deviating into other roles, such as counselor or legal adviser.

Members on the authorized interpreter list must receive refresher training annually or they will be removed from the authorized interpreter list. This annual training should include language skills competency (including specialized terminology) and ethical considerations.

The Training Supervisor shall be responsible for coordinating the annual refresher training and will maintain a record of all training the interpreters have received.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Communications with Persons with Disabilities

334.1 PURPOSE AND SCOPE

This policy provides guidance to members when communicating with individuals with disabilities, including those who are deaf or hard of hearing, have impaired speech or vision, or are blind.

334.1.1 DEFINITIONS

Definitions related to this policy include:

Auxiliary aids - Tools used to communicate with people who have a disability or impairment. They include, but are not limited to, the use of gestures or visual aids to supplement oral communication; a notepad and pen or pencil to exchange written notes; a computer or typewriter; an assistive listening system or device to amplify sound; a teletypewriter (TTY) or videophones (video relay service or VRS); taped text; qualified readers; a qualified interpreter.

Disability or impairment - An individual who has or is regarded as being substantially limited in a major life activity, including hearing or sight. For hearing, this includes any person who is deaf or hard of hearing and includes those who experience hearing losses ranging from a mild hearing loss to a profound hearing loss. For sight, this includes any person who cannot see without assistance from other than ordinary eyeglasses or contacts and any person whose blindness has been certified by a duly licensed physician or optometrist (42 USC § 12101; Va. Code § 51.5-111; Va. Code § 51.5-60).

Qualified interpreter - A person who is able to interpret effectively, accurately and impartially, both receptively and expressively, using any necessary specialized vocabulary. Qualified interpreters include oral interpreters, transliterators, sign language interpreters and intermediary interpreters.

334.2 POLICY

It is the policy of the Madison County Sheriff's Office to reasonably ensure that people with disabilities, including victims, witnesses, suspects and arrestees, have equal access to law enforcement services, programs and activities. Members must make efforts to communicate effectively with individuals with disabilities.

The Department will not discriminate against or deny any individual access to services, rights or programs based upon disabilities.

334.3 AMERICANS WITH DISABILITIES (ADA) COORDINATOR

The Sheriff shall delegate certain responsibilities to an ADA coordinator (28 CFR 35.107). The coordinator shall be appointed by and directly responsible to the Patrol Division Supervisor or the authorized designee.

The responsibilities of the coordinator include, but are not limited to:

(a) Working with the County ADA coordinator regarding the Madison County Sheriff's Office’s efforts to ensure equal access to services, programs and activities.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Developing reports or new procedures or recommending modifications to this policy.

(c) Acting as a liaison with local disability advocacy groups or other disability groups regarding access to department services, programs and activities.

(d) Ensuring that a list of qualified interpreter services is maintained and available to each Shift Supervisor and Dispatch Supervisor. The list should include information regarding:

1. Contact information.
2. Availability.

(e) Developing procedures that will enable members to access auxiliary aids or services, including qualified interpreters, and ensure the procedures are available to all members.

(f) Ensuring signage is posted in appropriate areas indicating that auxiliary aids are available free of charge to individuals with disabilities.

(g) Ensuring appropriate processes are in place to provide for the prompt and equitable resolution of complaints and inquiries regarding discrimination in access to department services, programs and activities.

334.4 FACTORS TO CONSIDER

Because the nature of any law enforcement contact may vary substantially from one situation to the next, members of this department should consider all information reasonably available to them when determining how to communicate with an individual with a disability. Members should carefully balance all known factors in an effort to reasonably ensure people who are disabled have equal access to services, programs and activities. These factors may include, but are not limited to:

(a) Members should not always assume that effective communication is being achieved. The fact that an individual appears to be nodding in agreement does not always mean he/she completely understands the message. When there is any doubt, members should ask the individual to communicate back or otherwise demonstrate his/her understanding.

(b) The nature of the disability (e.g., deafness or blindness vs. hard of hearing or low vision).

(c) The nature of the law enforcement contact (e.g., emergency vs. non-emergency, custodial vs. consensual contact).

(d) The availability of auxiliary aids. The fact that a particular aid is not available does not eliminate the obligation to reasonably ensure access. However, in an emergency, availability may factor into the type of aid used.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

334.5 INITIAL AND IMMEDIATE CONSIDERATIONS

Recognizing that various law enforcement encounters may be potentially volatile and/or emotionally charged, members should remain alert to the possibility of communication problems.

Members should exercise special care in the use of all gestures and verbal and written communication to minimize initial confusion and misunderstanding when dealing with any individual with known or suspected disabilities.

In a non-emergency situation, when a member knows or suspects an individual requires assistance to effectively communicate, the member shall identify the individual’s choice of auxiliary aid or service.

The individual’s preferred communication method must be honored unless another effective method of communication exists under the circumstances (28 CFR 35.160).

Factors to consider when determining whether an alternative method is effective include:

(a) The methods of communication usually used by the individual.

(b) The nature, length and complexity of the communication involved.

(c) The context of the communication.

In emergency situations involving an imminent threat to the safety or welfare of any person, members may use whatever auxiliary aids and services reasonably appear effective under the circumstances. This may include, for example, exchanging written notes or using the services of a person who knows sign language but is not a qualified interpreter, even if the person who is deaf or hard of hearing would prefer a qualified sign language interpreter or another appropriate auxiliary aid or service. Once the emergency has ended, the continued method of communication should be reconsidered. The member should inquire as to the individual's preference and give primary consideration to that preference.

If an individual who is deaf, is hard of hearing or has impaired speech must be handcuffed while in the custody of the Madison County Sheriff's Office, consideration should be given, safety permitting, to placing the handcuffs in the front of the body to facilitate communication using sign language or writing.

334.6 TYPES OF ASSISTANCE AVAILABLE

Madison County Sheriff's Office members shall never refuse an available service to an individual with disabilities who is requesting assistance. The Department will not charge anyone to receive auxiliary aids, nor shall it require anyone to furnish their own auxiliary aid or service as a condition for receiving assistance. The Department will make every reasonable effort to provide equal access and timely assistance to disabled individuals through a variety of services.

Disabled individuals may choose to accept department-provided auxiliary aids or services or they may choose to provide their own.

Department-provided auxiliary aids or services may include, but are not limited to, the assistance methods described in this policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

334.7 AUDIO RECORDINGS AND ENLARGED PRINT

The Department may develop audio recordings to assist people who are blind or have a visual impairment with accessing important information. If such a recording is not available, members may read aloud from the appropriate form (e.g., a personnel complaint form) or provide forms with enlarged print.

334.8 QUALIFIED INTERPRETERS

A qualified interpreter may be needed in lengthy or complex transactions (e.g., interviewing a victim, witness, suspect or arrestee) if the individual to be interviewed normally relies on sign language or speechreading (lip-reading) to understand what others are saying. The qualified interpreter should not be a person with an interest in the case or the investigation. A person providing interpretation services may be required to establish the accuracy and trustworthiness of the interpretation in a court proceeding.

Qualified interpreters should be:

(a) Available within a reasonable amount of time but in no event longer than one hour if requested.

(b) Experienced in providing interpretation services related to law enforcement matters.

(c) Familiar with the use of VRS and/or video remote interpreting services.

(d) Certified in either American Sign Language (ASL) or Signed English (SE).

(e) Able to understand and adhere to the interpreter role without deviating into other roles, such as counselor or legal adviser.

(f) Knowledgeable of the ethical issues involved when providing interpreter services.

Members should use department-approved procedures to request a qualified interpreter at the earliest reasonable opportunity, and generally not more than 15 minutes after a request for an interpreter has been made or it is reasonably apparent that an interpreter is needed. No individual who is disabled shall be required to provide his/her own interpreter (28 CFR 35.160).

334.9 TTY AND RELAY SERVICES

In situations where an individual without a disability would have access to a telephone (e.g., booking, attorney contacts), members must also provide those who are deaf, are hard of hearing or have impaired speech the opportunity to place calls using an available TTY (also known as a telecommunications device for deaf people, or TDD). Members shall provide additional time, as needed, for effective communication due to the slower nature of TTY and TDD communications.

The Department will accept all TTY or TDD calls placed by those who are deaf or hard of hearing and received via a telecommunications relay service (28 CFR 35.162).

Note that relay services translate verbatim, so the conversation must be conducted as if speaking directly to the caller.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

334.10 COMMUNITY VOLUNTEERS

Interpreter services may be available from community volunteers who have demonstrated competence in communication services, such as ASL or SE, and have been approved by the Department to provide interpreter services.

Where qualified interpreters are unavailable to assist, approved community volunteers who have demonstrated competence may be called upon when appropriate. However, department members must carefully consider the nature of the contact and the relationship between the individual with the disability and the volunteer to ensure that the volunteer can provide neutral and unbiased assistance.

334.11 FAMILY AND FRIENDS

While family or friends may offer to assist with interpretation, members should carefully consider the circumstances before relying on such individuals. The nature of the contact and relationship between the individual with the disability and the person offering services must be carefully considered (e.g., victim/suspect).

Children shall not be relied upon except in emergency or critical situations when there is no qualified interpreter reasonably available.

Adults may be relied upon when (28 CFR 35.160):

(a) There is an emergency or critical situation and there is no qualified interpreter reasonably available.

(b) The person with the disability requests that the adult interpret or facilitate communication and the adult agrees to provide such assistance, and reliance on that adult for such assistance is reasonable under the circumstances.

334.12 REPORTING

Whenever any member of this department is required to complete a report or other documentation, and communication assistance has been provided, such services should be noted in the related report. Members should document the type of communication services utilized and whether the individual elected to use services provided by the Department or some other identified source. If the individual’s express preference is not honored, the member must document why another method of communication was used.

All written communications exchanged in a criminal case shall be attached to the report or placed into evidence.

334.13 FIELD ENFORCEMENT

Field enforcement will generally include such contacts as traffic stops, pedestrian stops, serving warrants and restraining orders, crowd/traffic control and other routine field contacts that may involve individuals with disabilities. The scope and nature of these activities and contacts will inevitably vary.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

The Department recognizes that it would be virtually impossible to provide immediate access to complete communication services to every member of this department. Members and/or supervisors must assess each situation and consider the length, complexity and importance of the communication, as well as the individual's preferred method of communication, when determining the type of resources to use and whether a qualified interpreter is needed.

Although not every situation can be addressed in this policy, it is important that members are able to effectively communicate the reason for a contact, the need for information and the meaning or consequences of any enforcement action. For example, it would be meaningless to verbally request consent to search if the deputy is unable to effectively communicate with an individual who is deaf or hard of hearing and requires communications assistance.

If available, deputies should obtain the assistance of a qualified interpreter before placing an individual with a disability under arrest. Individuals who are arrested and are assisted by service animals should be permitted to make arrangements for the care of such animals prior to transport.

334.13.1 FIELD RESOURCES

Examples of methods that may be sufficient for transactions, such as checking a license or giving directions to a location or for urgent situations such as responding to a violent crime in progress, may, depending on the circumstances, include such simple things as:

(a) Hand gestures or visual aids with an individual who is deaf, is hard of hearing or has impaired speech.

(b) Exchange of written notes or communications.

(c) Verbal communication with an individual who can speech read by facing the individual and speaking slowly and clearly.

(d) Use of computer, word processing, personal communication device or similar device to exchange texts or notes.

(e) Slowly and clearly speaking or reading simple terms to individuals who have a visual or mental impairment.

Members should be aware that these techniques may not provide effective communication as required by law and this policy depending on the circumstances.

334.14 CUSTODIAL INTERROGATIONS

In an effort to ensure that the rights of individuals who are deaf, are hard of hearing, or have speech impairment are protected during a custodial interrogation, this department will provide interpreter services before beginning an interrogation, unless exigent circumstances exist or the individual has made a clear indication that the individual understands the process and desires to proceed without an interpreter. The use of a video remote interpreting service should be considered, where appropriate, if a live interpreter is not available. *Miranda* warnings shall be provided to suspects who are deaf or hard of hearing by a qualified interpreter or by providing a written *Miranda* warning card.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

To ensure that communications during custodial investigations are accurately documented and are admissible as evidence, interrogations should be recorded as required by law. See guidance on recording custodial interrogations in the Investigation and Prosecution Policy.

334.15 ARRESTS AND BOOKINGS

If an individual with speech or hearing disabilities is arrested, the arresting deputy shall use department-approved procedures to provide a qualified interpreter at the place of arrest or booking as soon as reasonably practicable, unless the individual indicates that he/she prefers a different auxiliary aid or service or the deputy reasonably determines another effective method of communication exists under the circumstances.

When gathering information during the booking process, members should remain alert to the impediments that often exist when communicating with those who are deaf, are hard of hearing, have impaired speech or vision, are blind or have other disabilities. In the interest of the arrestee's health and welfare, to protect the safety and security of the facility and to protect individual rights, it is important that accurate medical screening and booking information be obtained. If necessary, members should seek the assistance of a qualified interpreter whenever there is concern that accurate information cannot be obtained or that booking instructions may not be properly understood by the individual.

Individuals who require and possess personally owned communication aids (e.g., hearing aids, cochlear processors) should be permitted to retain them while in custody.

334.16 COMPLAINTS

The Department shall ensure that individuals with disabilities who wish to file a complaint regarding members of this department are able to do so. The Department may provide a qualified interpreter or forms in enlarged print, as appropriate. Complaints will be referred to the ADA coordinator.

Investigations into such complaints shall be handled in accordance with the Personnel Complaints Policy. Qualified interpreters used during the investigation of a complaint should not be members of this department.

334.17 COMMUNITY OUTREACH

Community outreach programs and other such services offered by this department are important to the ultimate success of more traditional law enforcement duties. This department will continue to work with community groups, local businesses and neighborhoods to provide equal access to such programs and services.

334.18 TRAINING

To ensure that all members who may have contact with disabled individuals are properly trained, the Department will provide periodic training that should include:

(a) Awareness and understanding of this policy and related procedures, related forms and available resources.

(b) Procedures for accessing qualified interpreters and other available resources.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) Working with in-person and telephone interpreters and related equipment.

The Training Supervisor shall be responsible for ensuring new members receive training related to interacting with individuals who have disabilities, including those who are deaf, are hard of hearing, have impaired speech or vision or are blind. Those who may have contact with such individuals should receive refresher training at least once every two years thereafter. The Training Supervisor shall maintain records of all training provided and will retain a copy in each member's training file in accordance with the established records retention schedule.

334.18.1 CALL-TAKER TRAINING

Emergency call-takers shall be trained in the use of TTY equipment protocols for communicating with individuals who are deaf, are hard of hearing or have speech impairments. Such training and information should include:

(a) The requirements of the ADA and Section 504 of the Rehabilitation Act for telephone emergency service providers.

(b) ASL syntax and accepted abbreviations.

(c) Practical instruction on identifying and processing TTY or TDD calls, including the importance of recognizing silent TTY or TDD calls and using proper syntax, abbreviations and protocol when responding to TTY or TDD calls.

(d) Hands-on experience in TTY and TDD communications, including identification of TTY or TDD tones.

Training should be mandatory for all the Dispatch Center members who may have contact with individuals from the public who are deaf, are hard of hearing or have impaired speech. Refresher training should occur every six months.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Mandatory Employer Notification

335.1 PURPOSE AND SCOPE

The purpose of this policy is to describe the notification requirements and procedures to follow when a public school employee (teacher and non-teacher) has been arrested under certain circumstances.

335.2 POLICY

The Madison County Sheriff's Office will meet the reporting mandates of Va. Code § 19.2-83.1 to minimize the risk to children and others.

335.3 MANDATORY NOTIFICATION

In the event a school employee is arrested for a felony or a Class 1 misdemeanor, or an equivalent offense in another state, a deputy shall file a report of such arrest with the designated school official of the employing school division by certified mail, return receipt requested, or by fax and email, as soon as practicable but no later than 48 hours following the arrest (Va. Code § 19.2-83.1).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Biological Samples

336.1 PURPOSE AND SCOPE

This policy provides guidelines for the collection of biological samples from those individuals required to provide samples upon conviction or arrest for certain offenses. This policy does not apply to biological samples collected at a crime scene or taken from an individual in conjunction with a criminal investigation, nor does it apply to biological samples collected from those required to register, for example, as sex offenders.

336.2 POLICY

The Madison County Sheriff's Office will assist in the expeditious collection of required biological samples from arrestees and offenders in accordance with the laws of this state and with as little reliance on force as practicable.

336.3 ARRESTEES AND OFFENDERS SUBJECT TO BIOLOGICAL SAMPLE COLLECTION

The following arrestees or offenders must submit a biological sample:

(a) Persons convicted of a felony or any qualifying violation as set forth in Va. Code § 19.2-310.2.

(b) Persons arrested for the commission or attempted commission of a violent felony as defined by Va. Code § 19.2-297.1 after a probable cause hearing has been held.

(c) Persons arrested for any qualifying violation as set forth in Va. Code § 19.2-310.2:1 after a probable cause hearing has been held.

336.4 PROCEDURE

When an arrestee or an offender is required to provide a biological sample, a trained member shall attempt to obtain the sample in accordance with this policy.

336.4.1 COLLECTION

The following steps should be taken to collect a sample:

(a) Verify that the arrestee or offender is required to provide a sample pursuant to Va. Code § 19.2-310.2 or Va. Code § 19.2-310.2:1.

(b) Verify that a biological sample has not been previously collected from the arrestee or offender by querying the Virginia Department of Forensic Science (DFS) DNA data bank sample tracking system. There is no need to obtain a biological sample if one has been previously obtained.

(c) Use the designated collection kit specified and distributed by the DFS to perform the collection and take steps to avoid cross contamination.

1. Offenders may have a blood, saliva, or tissue sample taken. Only a correctional health nurse technician, physician, registered nurse, or licensed practical nurse, graduate laboratory technician, or phlebotomist may withdraw a blood sample (Va. Code § 19.2-310.3).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. Arrestees may have a saliva or tissue sample taken (Va. Code § 19.2-310.3:1).

(d) Make a corresponding entry into the data bank sample tracking system and forward the sealed and appropriately labeled sample to DFS within 15 days of collection. Arrestee samples shall also include information identifying the arresting or accompanying officer, the offense for which the person was arrested, and a copy of the arrest warrant or capias (Va. Code § 19.2-310.3; Va. Code § 19.2-310.3:1).

336.5 USE OF FORCE TO OBTAIN SAMPLES

If an arrestee or offender refuses to cooperate with the sample collection process, members should attempt to identify the reason for refusal and seek voluntary compliance without resorting to using force. Force will not be used in the collection of samples except as authorized by court order or approval of legal counsel and only with the approval of the Captain.

Methods to consider when seeking voluntary compliance include contacting:

(a) The individual's parole or probation officer, when applicable.

(b) The prosecuting attorney to seek additional charges against the individual for failure to comply or to otherwise bring the refusal before a judge.

(c) The judge at the individual's next court appearance.

(d) The individual's attorney.

(e) A chaplain.

(f) Another custody facility with additional resources, where the individual can be transferred to better facilitate sample collection.

(g) A supervisor who may be able to authorize custodial disciplinary actions to compel compliance, if any are available.

The supervisor shall review and approve any plan to use force and be present to document the process.

336.5.1 VIDEO RECORDING

A video recording should be made any time force is used to obtain a biological sample. The recording should document all persons participating in the process, in addition to the methods and all force used during the collection. The recording should be part of the investigation file, if any, or otherwise retained in accordance with the established records retention schedule.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Chaplains

337.1 PURPOSE AND SCOPE

This policy establishes the guidelines for Madison County Sheriff's Office chaplains to provide counseling or emotional support to members of the Department, their families and members of the public.

337.2 POLICY

The Madison County Sheriff's Office shall ensure that department chaplains are properly appointed, trained and supervised to carry out their responsibilities without financial compensation.

337.3 ELIGIBILITY

Requirements for participation as a chaplain for the Department may include, but are not limited to:

(a) Being above reproach, temperate, prudent, respectable, hospitable, able to teach, free from addiction to alcohol or other drugs, and free from excessive debt.

(b) Managing his/her household, family and personal affairs well.

(c) Having a good reputation in the community.

(d) Successful completion of an appropriate-level background investigation.

(e) A minimum of five years of successful counseling experience.

(f) Possession of a valid driver’s license.

The Sheriff may allow exceptions to these eligibility requirements based on organizational needs and the qualifications of the individual.

337.4 RECRUITMENT, SELECTION AND APPOINTMENT

The Madison County Sheriff's Office shall endeavor to recruit and appoint only those applicants who meet the high ethical, moral and professional standards set forth by this department.

All applicants shall be required to meet and pass the same pre-employment procedures as department personnel before appointment.

337.4.1 RECRUITMENT

Chaplains should be recruited on a continuous and ongoing basis consistent with department policy on equal opportunity and non-discriminatory employment. A primary qualification for participation in the application process should be an interest in and an ability to assist the Department in serving the public. Chaplain candidates are encouraged to participate in ride-alongs with department members before and during the selection process.

337.4.2 SELECTION AND APPOINTMENT

Chaplain candidates shall successfully complete the following process prior to appointment as a chaplain:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) Submit the appropriate written application.

(b) Include a recommendation from employers or volunteer programs.

(c) Interview with the Sheriff and the chaplain coordinator.

(d) Successfully complete an appropriate-level background investigation.

(e) Complete an appropriate probationary period as designated by the Sheriff.

Chaplains are volunteers and serve at the discretion of the Sheriff. Chaplains shall have no property interest in continued appointment. However, if a chaplain is removed for alleged misconduct, the chaplain will be afforded an opportunity solely to clear his/her name through a liberty interest hearing, which shall be limited to a single appearance before the Sheriff or the authorized designee.

337.5 IDENTIFICATION AND UNIFORMS

As representatives of the Department, chaplains are responsible for presenting a professional image to the community. Chaplains shall dress appropriately for the conditions and performance of their duties. Uniforms and necessary safety equipment will be provided for each chaplain. Identification symbols worn by chaplains shall be different and distinct from those worn by deputies through the inclusion of "Chaplain" on the uniform. Chaplain uniforms shall not reflect any religious affiliation.

Chaplains will be issued Madison County Sheriff's Office identification cards, which must be carried at all times while on-duty. The identification cards will be the standard Madison County Sheriff's Office identification cards, with the exception that “Chaplain” will be indicated on the cards. Chaplains shall be required to return any issued uniforms or department property at the termination of service.

Chaplains shall conform to all uniform regulations and appearance standards of this department.

337.6 CHAPLAIN COORDINATOR

The Sheriff shall delegate certain responsibilities to a chaplain coordinator. The coordinator shall be appointed by and directly responsible to the Administration Division Supervisor or the authorized designee.

The chaplain coordinator shall serve as the liaison between the chaplains and the Sheriff. The function of the coordinator is to provide a central coordinating point for effective chaplain management within the Department, and to direct and assist efforts to jointly provide more productive chaplain services. Under the general direction of the Sheriff or the authorized designee, chaplains shall report to the chaplain coordinator and/or Shift Supervisor.

The chaplain coordinator may appoint a senior chaplain or other designee to assist in the coordination of chaplains and their activities.

The responsibilities of the coordinator or the authorized designee include, but are not limited to:

(a) Recruiting, selecting and training qualified chaplains.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Conducting chaplain meetings.

(c) Establishing and maintaining a chaplain callout roster.

(d) Maintaining records for each chaplain.

(e) Tracking and evaluating the contribution of chaplains.

(f) Maintaining a record of chaplain schedules and work hours.

(g) Completing and disseminating, as appropriate, all necessary paperwork and information.

(h) Planning periodic recognition events.

(i) Maintaining a liaison with other agency chaplain coordinators.

An evaluation of the overall use of chaplains will be conducted on an annual basis by the coordinator.

337.7 DUTIES AND RESPONSIBILITIES

Chaplains assist the Department, its members and the community as needed. Assignments of chaplains will usually be to augment the Patrol Division, but chaplains may be assigned to other areas within the Department as needed. Chaplains should be placed only in assignments or programs that are consistent with their knowledge, skills and abilities and the needs of the Department.

All chaplains will be assigned to duties by the chaplain coordinator or the authorized designee.

Chaplains may not proselytize or attempt to recruit members of the Department or the public into a religious affiliation while representing themselves as chaplains with this department. If there is any question as to the receiving person’s intent, chaplains should verify that the person is desirous of spiritual counseling or guidance before engaging in such discussion.

Chaplains may not accept gratuities for any service, or any subsequent actions or follow-up contacts that were provided while functioning as a chaplain for the Madison County Sheriff's Office.

337.7.1 COMPLIANCE

Chaplains are volunteer members of this department and, except as otherwise specified within this policy, are required to comply with the Volunteers Policy and other applicable policies.

337.7.2 OPERATIONAL GUIDELINES

(a) At the end of each watch the chaplain will complete a chaplain shift report and submit it to the Sheriff or the authorized designee.

(b) Chaplains shall be permitted to ride with deputies during any shift and observe Madison County Sheriff's Office operations, provided the Shift Supervisor has been notified and has approved the activity.

(c) Chaplains shall not be evaluators of members of the Department.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) In responding to incidents, a chaplain shall never function as a deputy.

(e) When responding to in-progress calls for service, chaplains may be required to stand by in a secure area until the situation has been deemed safe.

(f) Chaplains shall serve only within the jurisdiction of the Madison County Sheriff's Office unless otherwise authorized by the Sheriff or the authorized designee.

(g) Each chaplain shall have access to current department member rosters, addresses, telephone numbers, duty assignments, and other information that may assist in his/her duties. Such information will be considered confidential and each chaplain will exercise appropriate security measures to prevent unauthorized access to the data.

337.7.3 ASSISTING DEPARTMENT MEMBERS

The responsibilities of a chaplain related to department members include, but are not limited to:

(a) Assisting in making notification to families of members who have been seriously injured or killed and, after notification, responding to the hospital or home of the member.

(b) Visiting sick or injured members in the hospital or at home.

(c) Attending and participating, when requested, in funerals of active or retired members.

(d) Serving as a resource for members who are dealing with the public during significant incidents (e.g., accidental deaths, suicides, suicidal subjects, serious accidents, drug and alcohol abuse).

(e) Providing counseling and support for members and their families.

(f) Being alert to the needs of members and their families.

337.7.4 ASSISTING THE DEPARTMENT

The responsibilities of a chaplain related to this department include, but are not limited to:

(a) Assisting members in defusing a conflict or incident, when requested.

(b) Responding to any significant incident (e.g., natural and accidental deaths, suicides and attempted suicides, family disturbances) in which the Shift Supervisor or supervisor believes the chaplain could assist in accomplishing the mission of the Department.

(c) Responding to all major disasters, such as natural disasters, bombings and similar critical incidents.

(d) Being on-call and, if possible, on-duty during major demonstrations or any public function that requires the presence of a large number of department members.

(e) Attending department and academy graduations, ceremonies and social events and offering invocations and benedictions, as requested.

(f) Participating in in-service training classes.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(g) Training others to enhance the effectiveness of the Department.

337.7.5 ASSISTING THE COMMUNITY

The duties of a chaplain related to the community include, but are not limited to:

(a) Fostering familiarity with the role of law enforcement in the community.

(b) Providing an additional link between the community, other chaplain coordinators and the Department.

(c) Providing a liaison with various civic, business and religious organizations.

(d) Assisting the community when they request representatives or leaders of various denominations.

(e) Assisting the community in any other function, as needed or requested.

(f) Making referrals in cases where specialized attention is needed or in cases that are beyond the chaplain's ability to assist.

337.7.6 CHAPLAIN MEETINGS

All chaplains are required to attend scheduled meetings. Any absences must be satisfactorily explained to the chaplain coordinator.

337.8 PRIVILEGED COMMUNICATIONS

No person who provides chaplain services to members of the Department may work or volunteer for the Madison County Sheriff's Office in any capacity other than that of chaplain.

Department chaplains shall be familiar with state evidentiary laws and rules pertaining to the limits of the clergy-penitent, psychotherapist-patient and other potentially applicable privileges and shall inform members when it appears reasonably likely that the member is discussing matters that are not subject to privileged communications. In such cases, the chaplain should consider referring the member to a non-department counseling resource.

No chaplain shall provide counsel to or receive confidential communications from any Madison County Sheriff's Office member concerning an incident personally witnessed by the chaplain or concerning an incident involving the chaplain.

337.9 TRAINING

The Department will establish a minimum number of training hours and standards for department chaplains. The training, as approved by the Training Supervisor, may include:

- Stress management
- Death notifications
- Symptoms of post-traumatic stress
- Burnout for members of law enforcement and chaplains
- Legal liability and confidentiality

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Chaplains

- Ethics
- Responding to crisis situations
- The law enforcement family
- Substance abuse
- Deputy injury or death
- Sensitivity and diversity

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Child and Dependent Adult Safety

338.1 PURPOSE AND SCOPE

This policy provides guidelines to ensure that children and dependent adults are not left without appropriate care in the event their caregiver or guardian is arrested or otherwise prevented from providing care due to actions taken by members of this department.

This policy does not address the actions to be taken during the course of a child abuse or dependent adult investigation. These are covered in the Child Abuse and Adult Abuse policies.

338.2 POLICY

It is the policy of this department to mitigate, to the extent reasonably possible, the stressful experience individuals may have when their parent or caregiver is arrested. The Madison County Sheriff's Office will endeavor to create a strong, cooperative relationship with local, state and community-based social services to ensure an effective, collaborative response that addresses the needs of those affected, including call-out availability and follow-up responsibilities.

338.3 PROCEDURES DURING AN ARREST

When encountering an arrest or prolonged detention situation, deputies should make reasonable attempts to determine if the arrestee is responsible for children or dependent adults. In some cases this may be obvious, such as when children or dependent adults are present. However, deputies should inquire if the arrestee has caregiver responsibilities for any children or dependent adults who are without appropriate supervision. The following steps should be taken:

(a) Inquire about and confirm the location of any children or dependent adults.

(b) Look for evidence of children and dependent adults. Deputies should be mindful that some arrestees may conceal the fact that they have a dependent for fear the individual may be taken from them.

(c) Consider inquiring of witnesses, neighbors, friends and relatives of the arrestee as to whether the person is responsible for a child or dependent adult.

Whenever reasonably possible, deputies should consider reasonable alternatives to arresting a parent, guardian or caregiver in the presence of his/her child or dependent adult.

Whenever it is safe to do so, deputies should allow the parent or caregiver to assure children or dependent adults that they will be provided care. If this is not safe or if the demeanor of the parent or caregiver suggests this conversation would be nonproductive, the deputy at the scene should explain the reason for the arrest in age-appropriate language and offer reassurance to the child or dependent adult that he/she will receive appropriate care.

338.3.1 AFTER AN ARREST

Whenever an arrest is made, the deputy should take all reasonable steps to ensure the safety of the arrestee’s disclosed or discovered children or dependent adults.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Child and Dependent Adult Safety

Deputies should allow the arrestee reasonable time to arrange for care of children and dependent adults. Temporary placement with family or friends may be appropriate. However, any decision should give priority to a care solution that is in the best interest of the child or dependent adult. In such cases the following guidelines should be followed:

(a) Allow the person reasonable time to arrange for the care of children and dependent adults with a responsible party, as appropriate.

1. Deputies should consider allowing the person to use his/her cell phone to facilitate arrangements through access to contact phone numbers, and to lessen the likelihood of call screening by the recipients due to calls from unknown sources.

(b) Unless there is evidence that it would not be in the dependent person's best interest (e.g., signs of abuse, drug use, unsafe environment), deputies should respect the parent or caregiver's judgment regarding arrangements for care. It is generally best if the child or dependent adult remains with relatives or family friends that he/she knows and trusts because familiarity with surroundings and consideration for comfort, emotional state and safety are important.

1. Except when a court order exists limiting contact, the deputy should attempt to locate and place children or dependent adults with the non-arrested parent, guardian or caregiver.

(c) Provide for the immediate supervision of children or dependent adults until an appropriate caregiver arrives.

(d) Notify Child Protective Services (CPS) or Adult Protective Services (APS), if appropriate.

(e) Notify the field supervisor or Shift Supervisor of the disposition of children or dependent adults.

If children or dependent adults are at school or another known location outside the household at the time of arrest, the arresting deputy should attempt to contact the school or other known location and inform the principal or appropriate responsible adult of the caregiver's arrest and of the arrangements being made for the care of the arrestee's dependent. The result of such actions should be documented in the associated report.

338.3.2 DURING THE BOOKING PROCESS

During the booking process, the arrestee should be allowed to make telephone calls to arrange for the care of any child or dependent adult in accordance with the Temporary Custody of Adults Policy.

If an arrestee is unable to arrange for the care of any child or dependent adult through this process, or circumstances prevent them from making such arrangements (e.g., their behavior prevents reasonable accommodations for making necessary calls), a supervisor should be contacted to

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

determine the appropriate steps to arrange for care. These steps may include additional telephone calls or contacting a local, county or state services agency.

338.3.3 REPORTING

(a) For all arrests where children are present or living in the household, the reporting member will document the following information:

1. Name
2. Sex
3. Age
4. Special needs (e.g., medical, mental health)
5. How, where and with whom or which agency the child was placed
6. Identities and contact information for other potential caregivers
7. Notifications made to other adults (e.g., schools, relatives)

(b) For all arrests where dependent adults are present or living in the household, the reporting member will document the following information:

1. Name
2. Sex
3. Age
4. Whether the person reasonably appears able to care for him/herself
5. Disposition or placement information if he/she is unable to care for him/herself

See attachment: 314 Checklist for Drug-Endangered Dependent Persons Investigations.pdf

338.3.4 SUPPORT AND COUNSELING REFERRAL

If, in the judgment of the handling deputies, the child or dependent adult would benefit from additional assistance, such as counseling services, contact with a victim advocate or a crisis response telephone number, the appropriate referral information may be provided.

338.4 DEPENDENT WELFARE SERVICES

Whenever an arrestee is unwilling or incapable of arranging for the appropriate care of any child or dependent adult, the handling deputy should contact the appropriate welfare service or other department-approved social service agency to determine whether protective custody is appropriate.

Only when other reasonable options are exhausted should a child or dependent adult be transported to the sheriff's facility, transported in a marked law enforcement vehicle or taken into formal protective custody.

Under no circumstances should a child or dependent adult be left unattended or without appropriate care.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

338.5 TRAINING

The Training Supervisor is responsible for ensuring that all members of this department who may be involved in arrests affecting children or dependent adults receive approved training on effective safety measures when a parent, guardian or caregiver is arrested.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Service Animals

339.1 PURPOSE AND SCOPE

The purpose of this policy is to provide the guidelines necessary to ensure that the rights of individuals who use service animals to assist with disabilities are protected in accordance with Title II of the Americans with Disabilities Act (ADA).

339.1.1 DEFINITIONS

Definitions related to this policy include:

Service animal - A dog that is trained to do work or perform tasks for the benefit of an individual with a disability, including a physical, sensory, psychiatric, intellectual or other mental disability. The work or tasks performed by a service animal must be directly related to the individual's disability (28 CFR 35.104; Va. Code § 51.5-40.1).

Service animal also includes a miniature horse if the horse is trained to do work or perform tasks for people with disabilities, provided the horse is housebroken, is under the handler’s control, the facility can accommodate the horse’s type, size and weight, and the horse’s presence will not compromise legitimate safety requirements necessary for safe operation of the facility (28 CFR 35.136(i)).

339.2 POLICY

It is the policy of the Madison County Sheriff's Office to provide services and access to persons with service animals in the same manner as those without service animals. Department members shall protect the rights of persons assisted by service animals in accordance with state and federal law.

339.3 IDENTIFICATION AND USE OF SERVICE ANIMALS

Some service animals may be readily identifiable. Service animals may have a harness, backpack or vest identifying them as service animals Trained service dogs may assist individuals who are (Va. Code § 51.5-44):

(a) Partially or totally blind and the trained service dog may wear a harness.

(b) Deaf or hearing impaired and the trained service dog may wear a blaze orange leash.

(c) Mobility-impaired or otherwise disabled.

However, many service animals do not have a distinctive symbol, harness or collar.

Service animals may be used in a number of ways to provide assistance, including:

- Guiding people who are blind or have low vision.
- Alerting people who are deaf or hard of hearing.
- Retrieving or picking up items, opening doors or flipping switches for people who have limited use of their hands, arms or legs.
- Pulling wheelchairs.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

- Providing physical support and assisting with stability and balance.
- Doing work or performing tasks for persons with traumatic brain injury, intellectual disabilities or psychiatric disabilities, such as reminding a person with depression to take medication.
- Alerting a person with anxiety to the onset of panic attacks, providing tactile stimulation to calm a person with post-traumatic stress disorder, assisting people with schizophrenia to distinguish between hallucinations and reality, and helping people with traumatic brain injury to locate misplaced items or follow daily routines.

339.4 MEMBER RESPONSIBILITIES

Service animals that are assisting individuals with disabilities are permitted in all public facilities and areas where the general public is allowed. Department members are expected to treat individuals with service animals with the same courtesy and respect that the Madison County Sheriff's Office affords to all members of the public (28 CFR 35.136).

339.4.1 INQUIRY

If it is apparent or if a member is aware that an animal is a service animal, the individual generally should not be asked any questions as to the status of the animal. If it is unclear whether an animal meets the definition of a service animal, the member should ask the individual only the following questions (28 CFR 35.136(f)):

- Is the animal required because of a disability?
- What task or service has the service animal been trained to perform?

If the individual explains that the animal is required because of a disability and has been trained to work or perform at least one task, the animal meets the definition of a service animal and no further questions as to the animal's status should be asked. The individual should not be questioned about his/her disability nor should the person be asked to provide any license, certification or identification card for the service animal.

339.4.2 CONTACT

Service animals are not pets. Department members should not interfere with the important work performed by a service animal by talking to, petting or otherwise initiating contact with a service animal.

339.4.3 REMOVAL

If a service animal is not housebroken or exhibits vicious behavior, poses a direct threat to the health of others, or unreasonably disrupts or interferes with normal business operations, a deputy may direct the handler to remove the animal from the premises. Barking alone is not a threat nor does a direct threat exist if the person takes prompt, effective action to control the service animal (28 CFR 35.136(b)).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Each incident must be considered individually and past incidents alone are not cause for excluding a service animal. Removal of a service animal may not be used as a reason to refuse service to an individual with disabilities. Members of this department are expected to provide all services that are reasonably available to an individual with a disability, with or without a service animal.

339.4.4 COMPLAINTS

When handling calls of a complaint regarding a service animal, members of this department should remain neutral and should be prepared to explain the ADA requirements concerning service animals to the concerned parties. Businesses are required to allow service animals to accompany their handlers into the same areas that other customers or members of the public are allowed (28 CFR 36.302).

Absent a violation of law independent of the ADA, deputies should take no enforcement action beyond keeping the peace. Individuals who believe they have been discriminated against as a result of a disability should be referred to the Civil Rights Division of the U.S. Department of Justice (DOJ).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Volunteers

340.1 PURPOSE AND SCOPE

This policy establishes the guidelines for Madison County Sheriff's Office volunteers to supplement and assist department personnel in their duties. Trained volunteers are members who can augment department personnel and help complete various tasks.

340.1.1 DEFINITIONS

Definitions related to this policy include:

Volunteer - An individual who performs a service for the Department without promise, expectation or receipt of compensation for services rendered. This may include unpaid chaplains, unpaid reserve deputies, interns, persons providing administrative support, and youth involved in a law enforcement Explorer Post, among others.

340.2 POLICY

The Madison County Sheriff's Office shall ensure that volunteers are properly appointed, trained and supervised to carry out specified tasks and duties in order to create an efficient department and improve services to the community.

340.3 ELIGIBILITY

Requirements for participation as a volunteer for the Department may include, but are not limited to:

(a) Residency in the County of Madison County, Virginia.

(b) Being at least 18 years of age for all positions.

(c) Possession of a valid driver's license if the position requires vehicle operation.

(d) Possession of liability insurance for any personally owned equipment, vehicles or animals utilized during volunteer work.

(e) No conviction of a felony, any crime of a sexual nature or against children, any crime related to assault or violence, any crime related to dishonesty, or any crime related to impersonating a law enforcement officer.

(f) No conviction of a misdemeanor or gross misdemeanor crime within the past 10 years, excluding petty misdemeanor traffic offenses.

(g) No mental illness or chemical dependency condition that may adversely affect the person's ability to serve in the position.

(h) Ability to meet physical requirements reasonably appropriate to the assignment.

(i) A personal background history and character suitable for a person representing the Department, as validated by a background investigation.

The Sheriff may allow exceptions to these eligibility requirements based on organizational needs and the qualifications of the individual.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

340.4 RECRUITMENT, SELECTION AND APPOINTMENT

The Madison County Sheriff's Office shall endeavor to recruit and appoint only those applicants who meet the high ethical, moral and professional standards set forth by this department.

340.4.1 RECRUITMENT

Volunteers should be recruited on a continuous and ongoing basis consistent with department policy on equal opportunity, nondiscriminatory employment. A primary qualification for participation in the application process should be an interest in and an ability to assist the Department in serving the public.

Requests for volunteers should be submitted in writing by interested department members to the volunteer coordinator through the requester's immediate supervisor. A complete description of the volunteer's duties and a requested time frame should be included in the request. All department members should understand that the recruitment of volunteers is enhanced by creative and interesting assignments. The volunteer coordinator may withhold assignment of any volunteer until such time as the requester is prepared to make effective use of volunteer resources.

340.4.2 SELECTION

Volunteer candidates shall successfully complete the following process prior to appointment as a volunteer:

(a) Submit the appropriate written application.

(b) Interview with the volunteer coordinator.

(c) Successfully complete an appropriate-level background investigation.

340.4.3 APPOINTMENT

Service as a volunteer with the Department shall begin with an official notice of acceptance or appointment by the Sheriff or the authorized designee. Notice may only be given by an authorized representative of the Department, who will normally be the volunteer coordinator.

No volunteer should begin any assignment until he/she has been officially accepted for that position and has completed all required screening and paperwork. At the time of final acceptance, each volunteer should complete all required enrollment paperwork and will receive a copy of the position description and agreement of service with the Department.

All volunteers shall receive a copy of the volunteer orientation materials and shall be required to sign a volunteer agreement. Volunteers should be placed only in assignments or programs that are consistent with their knowledge, skills and abilities and the needs of the Department.

Volunteers serve at the discretion of the Sheriff.

340.5 IDENTIFICATION AND UNIFORMS

As representatives of the Department, volunteers are responsible for presenting a professional image to the community. Volunteers shall dress appropriately for the conditions and performance of their duties.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

340.6 PERSONNEL WORKING AS VOLUNTEERS

Qualified regular department personnel, when authorized, may also serve as volunteers. However, this department shall not utilize the services of volunteers in such a way that it would violate employment laws, county rule or policy (e.g., a detention deputy participating as a volunteer for reduced or no pay). Therefore, the volunteer coordinator should consult with the Human Resources Department prior to allowing regular department personnel to serve in a volunteer capacity (29 CFR 553.30).

340.7 VOLUNTEER COORDINATOR

The volunteer coordinator shall be appointed by and directly responsible to the Administration Division Supervisor or the authorized designee.

The function of the coordinator is to provide a central coordinating point for effective volunteer management within the Department, and to direct and assist efforts to jointly provide more productive volunteer services. Under the general direction of the Sheriff or the authorized designee, volunteers shall report to the volunteer coordinator and/or Shift Supervisor.

The volunteer coordinator may appoint a senior volunteer or other designee to assist in the coordination of volunteers and their activities.

The responsibilities of the coordinator or the authorized designee include, but are not limited to:

(a) Recruiting, selecting, and training qualified volunteers.

(b) Conducting volunteer meetings.

(c) Establishing and maintaining a volunteer callout roster.

(d) Maintaining records for each volunteer.

(e) Tracking and evaluating the contribution of volunteers.

(f) Maintaining a record of volunteer schedules and work hours.

(g) Completing and disseminating, as appropriate, all necessary paperwork and information.

(h) Planning periodic recognition events.

(i) Maintaining a liaison with other community programs that use volunteers and assisting in community-wide efforts to recognize and promote volunteering.

(j) Maintaining volunteer orientation and training materials and outlining expectations, policies, and responsibilities for all volunteers.

An evaluation of the overall use of volunteers will be conducted on an annual basis by the coordinator.

340.8 DUTIES AND RESPONSIBILITIES

Volunteers assist department personnel as needed. Assignments of volunteers will usually be to augment the Patrol Division, but volunteers may be assigned to other areas within the Department

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

as needed. Volunteers should be placed only in assignments or programs that are consistent with their knowledge, skills and abilities and the needs of the Department.

All volunteers will be assigned to duties by the volunteer coordinator or the authorized designee.

340.8.1 COMPLIANCE

Volunteers shall be required to adhere to all department policies and procedures. A copy of the policies and procedures will be made available to each volunteer upon appointment. The volunteer shall become thoroughly familiar with these policies.

Whenever a rule, regulation or guideline in this Policy Manual refers to regular department personnel, it shall also apply to a volunteer, unless by its nature it is inapplicable.

Volunteers are required by this department to meet department-approved training requirements as applicable to their assignments.

340.8.2 VOLUNTEER MEETINGS

All volunteers are required to attend scheduled meetings. Any absences must be satisfactorily explained to the volunteer coordinator.

340.9 TASK-SPECIFIC TRAINING

Task-specific training is intended to provide the required instruction and practice for volunteers to properly and safely perform their assigned duties. A volunteer’s training should correspond to his/her assignment as determined by the volunteer coordinator.

Volunteers will be provided with an orientation program to acquaint them with the policies of the Department and law enforcement procedures applicable to their assignments.

Volunteers should receive position-specific training to ensure they have adequate knowledge and skills to complete the required tasks, and should receive ongoing training as deemed appropriate by their supervisors or the volunteer coordinator.

Training should reinforce to volunteers that they shall not intentionally represent themselves as, or by omission infer that they are, deputies or other full-time members of the Department. They shall always represent themselves as volunteers.

All volunteers shall comply with the rules of conduct and with all applicable orders and directives, either oral or written, issued by the Department.

340.9.1 VOLUNTEER TRAINING MATERIALS

Each new volunteer will be issued volunteer training materials, as appropriate. The materials outline the subject matter and skills necessary to properly function as a volunteer with the Madison County Sheriff's Office. The volunteer shall become knowledgeable of the subject matter and proficient with the skills as set forth in the training materials.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

340.10 SUPERVISION

Each volunteer must have a clearly identified supervisor who is responsible for direct management of that volunteer. This supervisor will be responsible for day-to-day management and guidance of the work of the volunteer and should be available to the volunteer for consultation and assistance.

Functional supervision of volunteers is the responsibility of the supervisor in charge of the volunteer's assigned duties. The following are some considerations that supervisors should keep in mind while supervising volunteers:

(a) Take the time to introduce volunteers to members on all levels.

(b) Ensure volunteers have work space and necessary office supplies.

(c) Make sure the work is challenging. Do not hesitate to give volunteers an assignment or task that will utilize these valuable resources.

A volunteer may be assigned as a supervisor of other volunteers, provided that the supervising volunteer is under the direct supervision of an employee of the Madison County Sheriff's Office.

340.10.1 EVALUATIONS

While in training, volunteers should be continuously evaluated using standardized daily and weekly observation reports. A volunteer will be considered a trainee until he/she has satisfactorily completed training. Volunteers who have completed their training should be evaluated annually using performance dimensions applicable to the duties and authorities granted to that volunteer.

340.10.2 FITNESS FOR DUTY

No volunteer shall report for work or be at work when his/her judgment or physical condition has been impaired due to illness or injury, or by the use of alcohol or drugs, whether legal or illegal.

Volunteers shall report to their supervisors any change in status that may affect their ability to fulfill their duties. This includes, but is not limited to:

(a) Driver's license.

(b) Medical condition.

(c) Arrests.

(d) Criminal investigations.

(e) All law enforcement contacts.

340.11 INFORMATION ACCESS

With appropriate security clearance, a volunteer may have access to or be in the vicinity of criminal histories, investigative files or information portals. Unless otherwise directed by a supervisor, the duties of the position or department policy, all such information shall be considered confidential. Only that information specifically identified and approved by authorized members shall be released. Confidential information shall be given only to persons who have a need and a right to know as determined by department policy and supervisory personnel.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

A volunteer whose assignment requires the use of, or access to, confidential information will be required to have his/her fingerprints submitted to the Criminal Justice Information Services Divisions (CJIS) of the Virginia State Police to obtain clearance. Volunteers working this type of assignment will receive training in data practices and be required to sign a nondisclosure agreement before being given an assignment with the Department. Subsequent unauthorized disclosure of any confidential information verbally, in writing or by any other means by the volunteer is grounds for immediate dismissal and possible criminal prosecution.

Volunteers shall not address public gatherings, appear on radio or television, prepare any article for publication, act as correspondents to newspapers or other periodicals, release or divulge any information concerning the activities of the Department, or maintain that they represent the Department in such matters without permission from the proper department personnel.

340.11.1 RADIO AND MOBILE DATA COMPUTER USAGE

Volunteers shall successfully complete state and federal database access training and radio procedures training prior to using sheriff's radios or Mobile Data Computers and shall comply with all related provisions. The volunteer coordinator should ensure that radio and database access training is provided for volunteers whenever necessary.

340.12 EQUIPMENT

Any property or equipment issued by the Department shall be for official and authorized use only. Any property or equipment issued to a volunteer shall remain the property of the Department and shall be returned at the termination of service.

340.13 DISCIPLINARY PROCEDURES/TERMINATION

If a volunteer has a personnel complaint made against him/her or becomes involved in an internal investigation, the matter shall be investigated in compliance with the Personnel Complaints Policy.

Volunteers are considered at-will and may be removed from service at the discretion of the Sheriff, with or without cause. Volunteers shall have no property interest in their continued appointments. However, if a volunteer is removed for alleged misconduct, the volunteer will be afforded an opportunity solely to clear his/her name through a liberty interest hearing, which shall be limited to a single appearance before the Sheriff or the authorized designee.

Volunteers may resign from volunteer service with the Department at any time. It is requested that volunteers who intend to resign provide advance notice and a reason for their decision.

340.13.1 EXIT INTERVIEWS

The volunteer coordinator should conduct exit interviews, where possible. These interviews should ascertain why the volunteer is leaving the position and should solicit the volunteer’s suggestions on improving the position. When appropriate, an exit interview should also include a discussion on the possibility of involvement in some other capacity with the Department.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Native American Graves Protection and Repatriation

341.1 PURPOSE AND SCOPE

This policy is intended ensure the protection and security of ancient or historic grave sites, including notification of personnel responsible for cultural items, in compliance with the Native American Graves Protection and Repatriation Act (NAGPRA) (25 USC § 3001).

341.1.1 DEFINITIONS

Definitions related to this policy include (43 CFR 10.2):

Funerary objects and associated funerary objects - Objects that, as part of the death rite or ceremony of a culture, are reasonably believed to have been placed intentionally at the time of death or later with or near individual human remains, or that were made exclusively for burial purposes, or to contain human remains.

Native American human remains - The physical remains of the body of a person of Native American ancestry.

Objects of cultural patrimony - Objects having ongoing historical, traditional or cultural importance that is central to the Native American group or culture itself and therefore cannot be appropriated or conveyed by any individual, including members of the Native American group or Native Hawaiian organization. Such objects must have been considered inalienable by the Native American group at the time the object was separated from the group.

Sacred objects - Specific ceremonial objects needed by traditional Native American religious leaders for the practice of traditional Native American religions.

341.2 POLICY

It is the policy of the Madison County Sheriff's Office that the protection of Native American human remains, funerary objects, sacred objects or objects of cultural patrimony on federal lands is the responsibility of all members. Such protection includes minimizing destruction, contamination, inadvertent disruption or complicated custody transfer processes.

341.3 COMPLIANCE WITH THE NATIVE AMERICAN GRAVES PROTECTION AND REPATRIATION ACT

Upon discovery or arrival upon a scene where it reasonably appears that a Native American grave, human remains, funerary objects, sacred objects or objects of cultural patrimony are exposed or otherwise unsecured, members shall secure the site in the same manner as a crime scene. All activity at the scene other than scene preservation activity must cease (43 CFR 10.4).

No photography or video recording may be permitted by the media or any group or individual who may wish to exhibit the remains.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Without delay, the appropriate agency or group shall be notified to respond and take control of the scene. These include the following (43 CFR 10.4(d)):

- Federal land - Appropriate agency at the U.S. Department of the Interior or U.S. Department of Agriculture
- State land - Virginia Department of Historic Resources (Va. Code § 10.1-2300 et seq.)
- Tribal land - Responsible Indian tribal official

341.4 EVIDENCE AND PROPERTY

If the location has been investigated as a possible homicide scene prior to identification as a NAGPRA site, investigators shall work with other appropriate agencies and individuals to ensure the proper transfer and repatriation of any material collected. Members shall ensure that any remains or artifacts located at the site are expediently processed (43 CFR 10.6).

341.5 TREATMENT AND DISPOSITION OF HUMAN REMAINS

This department shall cooperate with other government agencies and the Virginia Department of Historic Resources to carry out any provisions of state law regarding treatment and disposition of human remains (Va. Code § 10.1-2300 et seq.).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Off-Duty Law Enforcement Actions

342.1 PURPOSE AND SCOPE

This policy is intended to provide guidelines for deputies of the Madison County Sheriff's Office with respect to taking law enforcement action while off-duty.

342.2 POLICY

It is the policy of the Madison County Sheriff's Office that deputies generally should not initiate law enforcement action while off-duty. Deputies are not expected to place themselves in unreasonable peril and should first consider reporting and monitoring the activity. However, any deputy who becomes aware of an incident or circumstance that he/she reasonably believes poses an imminent threat of serious bodily injury or death, or significant property damage or loss, may take reasonable action to minimize or eliminate the threat.

342.3 DECISION TO INTERVENE

There is no legal requirement for off-duty deputies to take law enforcement action. Deputies should consider waiting for on-duty uniformed law enforcement personnel to arrive instead of immediately intervening and, while waiting, gather as much accurate intelligence as possible. However, if a deputy decides to intervene, he/she must evaluate whether the action is necessary or desirable, and should take into consideration:

(a) The potential to be misidentified by other law enforcement personnel.

(b) The potential to be misidentified by members of the public, who may be armed or who may take action.

(c) The tactical disadvantage of being alone and the possibility of multiple or hidden suspects.

(d) Limited off-duty firearms capabilities and ammunition.

(e) The inability to communicate with responding law enforcement personnel.

(f) The lack of equipment, such as body armor, handcuffs or control devices.

(g) Unfamiliarity with the surroundings, including escape routes.

(h) The potential for increased risk to bystanders by confronting a suspect or taking action.

342.3.1 INTERVENTION PROCEDURE

If involvement is reasonably necessary, the deputy should attempt to call or have someone else call 9-1-1 to request immediate assistance. If possible, the dispatcher receiving the call should obtain a description of the off-duty deputy from the caller and broadcast that information to responding deputies.

Whenever practicable, the deputy should loudly and repeatedly identify him/herself as a deputy with the Madison County Sheriff's Office until acknowledged. Official identification should also be displayed when possible.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

342.4 CONSIDERATIONS

When encountering a non-uniformed deputy in public, uniformed deputies should wait for acknowledgement by the non-uniformed deputy in case he/she is working in an undercover capacity.

342.4.1 NON-SWORN RESPONSIBILITIES

Non-sworn members should not become involved in any law enforcement action while off-duty except to notify the local law enforcement authority and remain at the scene, if safe and practicable.

342.4.2 INCIDENTS OF PERSONAL INTEREST

Department members should refrain from handling incidents of personal interest (e.g., family or neighbor disputes) and should remain neutral. In such circumstances members should call the responsible agency to handle the matter.

342.5 REPORTING

If prior notification to the appropriate local law enforcement agency is not reasonably possible before taking action, the deputy shall notify the agency as soon as reasonably practicable. Deputies shall cooperate fully with the agency having jurisdiction by providing statements or reports as requested or as appropriate.

Deputies shall notify the Shift Supervisor who shall promptly notify the Sheriff regarding any law enforcement action taken while off-duty. The Shift Supervisor may send a supervisor to the location. The Sheriff may request assistance from the Internal Affairs Unit, if deemed appropriate.

The Shift Supervisor shall determine whether a crime report or an administrative report should be completed by the involved deputy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Human Trafficking

343.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the investigation of human trafficking. These guidelines will address unique aspects of such cases and minimize the effects that these crimes have on the victims.

343.1.1 DEFINITIONS

Definitions related to this policy include:

Force, fraud and coercion - Methods used by traffickers to press victims into lives of servitude and/or abuse.

- **Force** - Includes, but is not limited to, rape, beatings, burnings, constraint, confinement or deprivation (e.g., sleep, food and/or liquids, drug use).
- **Fraud** - Includes, but is not limited to, false and deceptive offers of employment, love/marriage or a better life.
- **Coercion** - A climate of fear which includes threats of serious harm to, or physical restraint of, any person; any scheme, plan or pattern intended to cause victims to believe that failure to perform an act would result in restraint and/or physical harm against them and/or their loved ones; or the abuse or threatened abuse of the legal process; creating dependency; establishing quotas.

Human trafficking - A modern-day form of slavery involving the illegal trade of people for exploitation or commercial gain. Crimes often related to human trafficking include:

(a) Taking or detaining a person for prostitution or consenting thereto (Va. Code § 18.2-355).

(b) Abduction and kidnapping (Va. Code § 18.2-47).

(c) Abduction with intent to extort money or for immoral purpose (Va. Code § 18.2-4).

(d) Receiving money from earnings of a male or female prostitute (Va. Code § 18.2-357).

Labor trafficking - The recruitment, harboring, transportation, provision or obtaining of a person for labor or services through the use of fraud or coercion for the purpose of involuntary servitude, peonage, debt bondage or slavery. This occurs in situations of forced labor such as domestic servitude, factory, construction, housekeeping, food service or agricultural work.

Sex trafficking - The recruitment, harboring, transportation, provision or obtaining of a person for the purpose of a commercial sex act in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such act is under 18 years of age.

343.2 POLICY

It is the policy of the Madison County Sheriff's Office that its members, when responding to reports of human trafficking, will strive to identify and assist the victims of human trafficking, aggressively

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

investigate human trafficking offenses and effectively identify, apprehend and prosecute those engaged in trafficking offenses in cooperation with state and federal laws.

343.3 RESPONSE TO HUMAN TRAFFICKING INCIDENTS

343.3.1 THE DISPATCH CENTER RESPONSIBILITIES

When the Dispatch Center receives a call reporting a case of human trafficking, dispatchers communications personnel shall follow standard emergency response, which includes:

(a) Evaluating and properly prioritizing the call.

(b) Securing medical assistance when appropriate.

(c) Determining the current location of any suspects.

(d) Obtaining detailed information to identify any suspects.

(e) Obtaining information about the relationship between any suspects and any victims.

(f) Determining whether weapons are involved.

(g) Determining whether there is a history of violence.

(h) Determining whether there are unique hazards that may be presented to the suspects, victims, responding personnel or others.

Call prioritization should be based on actual or perceived injuries and harm and whether the suspect poses an imminent danger.

343.3.2 COMMUNICATING WITH VICTIMS OF HUMAN TRAFFICKING

Contact and communication with victims of human trafficking crimes are critical. Deputies should be aware of their behavior in interactions with human trafficking victims and understand that trust is generally the top priority in communicating with human trafficking victims.

(a) For the victim’s safety and to obtain his/her cooperation and trust, strict confidentiality is paramount to prosecuting human traffickers and getting the human trafficking victim the help he/she needs.

    1. Talk to the victim in a safe and confidential environment.

    2. Limit the number of deputies and/or staff members coming into contact with the suspected human trafficking victim.

(b) Deputies should indirectly and sensitively determine if a person is the victim of human trafficking and recognize that:

    1. The victim may deny being a human trafficking victim. Asking direct questions will not always be beneficial.

    2. The phrase "trafficking victim" may have no meaning to the victim or it may frighten the victim.

    3. As an investigator, the deputy should be on the victim’s level (e.g., positioning, language, tone and tenor of voice).

    4. Displays of emotion or surprise (e.g., gasps, acting shocked) are not appropriate.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

5. Pity, judgment or patronization are not appropriate
6. Negative behavior (e.g., victim-blaming attitude, body language or behavior) are not appropriate.

(c) Deputies should be cautious when they arrive on-scene. Locate the victim and determine if there is a language barrier. A translator should be called to the scene if needed or appropriate. Do not use anyone from the scene as a translator as this could be someone working for the suspected human trafficker. Notify a qualified department translator who has been trained on interviewing human trafficking victims as soon as practicable.

(d) If the human trafficking victim is a child, enlist a specialist trained in interviewing child human trafficking or abuse victims.

343.3.3 INITIAL VICTIM INTERVIEW ACTIONS

Human trafficking cases are time sensitive and interviews should be conducted upon initial response. The deputy should interview the human trafficking victim and record the answers to as many of the following questions as possible:

(a) Is the victim free to leave the work site?

(b) Has the victim has been physically, sexually or psychologically abused or involved with drug usage?

(c) Does the victim have a passport or valid identification card, and is he/she in possession of such documents?

(d) What is the pay and conditions of his/her employment?

(e) Does the victim live at home or at/near the work site?

(f) If the suspected victim is a foreign national, how did the victim travel and arrive at this destination?

(g) Has the victim or a family member of the victim been threatened?

(h) Does the victim fear that something bad will happen to him/her, a family member or another person if he/she leaves the job?

(i) Are there other potential victims on-scene?

(j) Is the suspected trafficker is on-scene and, if not, where is he/she?

343.3.4 DEPUTY RESPONSIBILITIES

Responding deputies should arrest the suspected human trafficker as authorized by law. Deputies should:

(a) Evaluate the scene.

(b) Provide aid and assistance as may be needed, including making arrangements for transporting any victims.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) Interview any victims (determining willingness to cooperate with an investigation if the person is an adult; however, other evidence may be used if a victim is unwilling), witnesses and suspects.

(d) Identify, record, collect and/or preserve physical evidence.

(e) Determine the offense and appropriate charges.

(f) Arrest the suspect.

(g) When the suspect is not on the scene and probable cause exists, the deputy should notify the Shift Supervisor and provide the appropriate information for broadcast of an alert bulletin.

(h) Make referrals for help services (i.e., Child Protective Services, social services, rape counseling, domestic and family violence shelters).

(i) Obtain an arrest warrant.

(j) Petition for an emergency protective order for victims.

(k) Serve any issued emergency protective order and deliver the order to the Dispatch Center, taking appropriate steps to have entered into Virginia Criminal Information Network (VCIN).

(l) Complete the appropriate report and ensure the human trafficking offense box is properly completed.

343.3.5 SHIFT SUPERVISOR RESPONSIBILITIES

In any case where the deputy has not made an arrest but there is probable cause and the suspect is not on the scene, the Shift Supervisor should ensure the broadcast of an alert bulletin is completed.

The Shift Supervisor should notify the Investigation Division supervisor on all trafficking cases.

343.3.6 INVESTIGATION DIVISION RESPONSIBILITIES

When notified, the Investigation Division supervisor should ensure that a member of the Investigation Division responds and initiates an investigation. If an arrest warrant can be issued, it should be done immediately and reasonable attempts should be made to locate and arrest the suspect.

(a) Often victims of labor and/or sex trafficking will cooperate more when an outside service provider is involved to assess immediate needs. If there are no services available on-scene to meet the basic needs of any victims they are likely to stay in crisis and not respond to law enforcement reliably.

(b) The Investigation Division should consider use of a language assistance tool similar to the Victim Translation Assistance Tool (VITA), created by the United Nations that allows communication with people speaking another language.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Community Relations

344.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for community relationship-building.

Additional guidance on community relations and outreach is provided in other policies, including the:

- Hate Crimes Policy.
- Limited English Proficiency Services Policy.
- Communications with Persons with Disabilities Policy.
- Chaplains Policy.
- Patrol Policy.
- Suspicious Activity Reporting Policy.

344.2 POLICY

It is the policy of the Madison County Sheriff's Office to promote positive relationships between department members and the community by treating community members with dignity and respect and engaging them in public safety strategy development and relationship-building activities, and by making relevant policy and operations information available to the community in a transparent manner.

344.3 MEMBER RESPONSIBILITIES

Deputies should, as time and circumstances reasonably permit:

(a) Make casual and consensual contacts with community members to promote positive community relationships (see the Contacts and Temporary Detentions Policy).

(b) Become reasonably familiar with the schools, businesses and community groups in their assigned jurisdictional areas.

(c) Work with community members and the department community relations coordinator to identify issues and solve problems related to community relations and public safety.

(d) Conduct periodic foot patrols of their assigned areas to facilitate interaction with community members. Deputies carrying out foot patrols should notify an appropriate supervisor and the Dispatch Center of their status (i.e., on foot patrol) and location before beginning and upon completion of the foot patrol. They should also periodically inform the Dispatch Center of their location and status during the foot patrol.

344.4 COMMUNITY RELATIONS COORDINATOR

The Sheriff or the authorized designee should designate a member of the Department to serve as the community relations coordinator. He/she should report directly to the Sheriff or the authorized designee and is responsible for:

(a) Obtaining department-approved training related to his/her responsibilities.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Responding to requests from department members and the community for assistance in identifying issues and solving problems related to community relations and public safety.

(c) Organizing surveys to measure the condition of the department's relationship with the community.

(d) Working with community groups, department members and other community resources to:

1. Identify and solve public safety problems within the community.
2. Organize programs and activities that help build positive relationships between department members and the community and provide community members with an improved understanding of department operations.

(e) Working with the Patrol Division Supervisor to develop patrol deployment plans that allow deputies the time to participate in community engagement and problem-solving activities.

(f) Recognizing department and community members for exceptional work or performance in community relations efforts.

(g) Attending County Board of Supervisors and other community meetings to obtain information on community relations needs.

(h) Assisting with the department's response to events that may affect community relations, such as an incident where the conduct of a department member is called into public question.

(i) Informing the Sheriff and others of developments and needs related to the furtherance of the department's community relations goals, as appropriate.

344.5 COMMUNITY AND YOUTH ACTIVITIES AND PROGRAMS

The community relations coordinator should organize or assist with programs and activities that create opportunities for department members and community members, especially youth, to interact in a positive setting. Examples of such programs and events include:

(a) Department-sponsored athletic programs (e.g., baseball, basketball, soccer, bowling).

(b) Police-community get-togethers (e.g., cookouts, meals, charity events).

(c) Youth leadership and life skills mentoring.

(d) School resource deputy/Drug Abuse Resistance Education (D.A.R.E.®) programs.

(e) Neighborhood Watch and crime prevention programs.

344.6 INFORMATION SHARING

The community relations coordinator should work with the Public Information Officer to develop methods and procedures for the convenient sharing of information (e.g., major incident notifications, significant changes in department operations, comments, feedback, positive events) between the Department and community members. Examples of information-sharing methods include:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) Community meetings.

(b) Social media (see the Department Use of Social Media Policy).

(c) Department website postings.

Information should be regularly refreshed, to inform and engage community members continuously.

344.7 LAW ENFORCEMENT OPERATIONS EDUCATION

The community relations coordinator should develop methods to educate community members on general law enforcement operations so they may understand the work that deputies do to keep the community safe. Examples of educational methods include:

(a) Development and distribution of informational cards/flyers.

(b) Department website postings.

(c) Presentations to driver education classes.

(d) Instruction in schools.

(e) Department ride-alongs (see the Ride-Alongs Policy).

(f) Scenario/Simulation exercises with community member participation.

(g) Youth internships at the Department.

(h) Citizen academies.

Instructional information should include direction on how community members should interact with the police during enforcement or investigative contacts and how community members can make a complaint to the Department regarding alleged misconduct or inappropriate job performance by department members.

344.8 SAFETY AND OTHER CONSIDERATIONS

Department members responsible for community relations activities should consider the safety of the community participants and, as much as reasonably practicable, should not allow them to be present in any location or situation that would jeopardize their safety.

Department members in charge of community relations events should ensure that participating community members have completed waiver forms before participation, if appropriate. A parent or guardian must complete the waiver form if the participating community member has not reached 18 years of age.

Community members are subject to a criminal history check before approval for participation in certain activities, such as citizen academies.

344.9 TRANSPARENCY

The Department should periodically publish statistical data and analysis regarding the department’s operations. The reports should not contain the names of deputies, suspects or case numbers. The community relations coordinator should work with the community

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

advisory committee to identify information that may increase transparency regarding department operations.

344.10 TRAINING

Subject to available resources, members should receive training related to this policy, including training on topics such as:

(a) Effective social interaction and communication skills.

(b) Cultural, racial and ethnic diversity and relations.

(c) Building community partnerships.

(d) Community policing and problem-solving principles.

(e) Enforcement actions and their effects on community relations.

Where practicable and appropriate, community members, especially those with relevant expertise, should be involved in the training to provide input from a community perspective.

344.11 CAMPUS SAFETY

The Sheriff should work with the local school board and area schools to enter into a memorandum of understanding for school resource [officers_deputies] when required by law and to identify campuses that do not employ a school resource deputy. The Sheriff should designate a deputy to each identified campus and provide training to the deputy as required by law (Va. Code § 22.1-280.2:3).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Substantial Risk Orders

345.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for petitioning for and serving substantial risk orders, and accounting for firearms obtained pursuant to those orders.

345.1.1 DEFINITIONS

Definitions related to this policy include (Va. Code § 19.2-152.13; Va. Code § 19.2-152.14)

Substantial risk order - An order prohibiting a named person from purchasing, possessing, or transporting a firearm.

Prohibited items - Firearms and concealed handgun permits that are prohibited by a substantial risk order.

345.2 POLICY

It is the policy of the Madison County, Virginia to petition for and serve substantial risk orders in compliance with state law, and to properly account for prohibited items obtained by the Department pursuant to such orders.

345.3 SUBSTANTIAL RISK ORDER COORDINATOR

The Sheriff will appoint a substantial risk order coordinator. The responsibilities of the coordinator include:

(a) Developing and maintaining procedures for the filing of a petition for an order or a renewal of an order by department members (Va. Code § 19.2-152.13).

(b) Developing and maintaining factors to consider when assessing the need to seek an order, including:

1. Whether threats have been made, and if so, whether the threats are credible and specific.
2. Whether the potential victim is within close proximity.
3. Whether the person has expressed suicidal tendencies.
4. Whether the person has access to firearms.
5. The criminal history of the person, in particular any history of criminal violence, including whether the person is currently on parole, probation, or monitored release.
6. The mental health history of the person, in particular whether the person has any history of mental illness or has ever been detained for being a danger to self or others.
7. Any upcoming holidays, anniversaries, or other dates of significance that may serve as a trigger for the person, such as the death of a family member.
8. Whether the person has any history of drug or alcohol abuse.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) Developing and maintaining procedures for the receipt and service of orders consistent with the requirements of Va. Code § 19.2-152.13 and Va. Code § 19.2-152.14. Procedures should include:

1. A process for the evaluation of an order to determine appropriate service and necessary precautions (see the Warrant Service Policy and the Operations Planning and Deconfliction Policy).
2. A process established in coordination with the Records Manager for the entry of orders into appropriate databases, notice to courts, and removal of orders from databases, as applicable (Va. Code § 19.2-152.13; Va. Code § 19.2-152.14).
3. A process for obtaining a search warrant for any firearms when there is reason to believe that a person has not relinquished all firearms pursuant to an order (Va. Code § 19.2-152.13; Va. Code § 19.2-152.14).

(d) Coordinating with the Training Manager to provide deputies who may be involved in petitioning for or serving orders with training on such orders. Training should include determining when a petition is appropriate, the process for seeking an order, and the service of such orders.

(e) Reviewing each petition, each affidavit, and any associated court documents for an order prepared by members, for compliance with this policy, departmentprocedures, and state law.

(f) Developing and maintaining procedures for members to accept voluntarily surrendered prohibited items at times other than when an order is being served by the department.

1. Procedures should include preparing and providing a receipt identifying all prohibited items to the person surrendering the items.

(g) Developing and maintaining procedures for releasing, disposing of, or transferring firearms after appropriate database checks (Va. Code § 19.2-152.14; Va. Code § 19.2-152.15).

345.4 SUBSTANTIAL RISK ORDERS

A deputy who reasonably believes that a substantial risk order is appropriate should obtain approval from an appropriate supervisor and the substantial risk order coordinator or authorized designee prior to seeking an order.

345.4.1 STANDARDS

Substantial risk orders may be appropriate when there is clear and convincing evidence to believe that a person poses a substantial risk of personal injury to self or others in the near future by possessing or acquiring a firearm (Va. Code § 19.2-152.14).

An emergency substantial risk order may be appropriate when there is probable cause to believe that a person poses a substantial risk of personal injury to self or others in the near future by possessing or acquiring a firearm (Va. Code § 19.2-152.13).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

345.4.2 REQUIREMENTS OF PETITION
An application for a substantial risk order should be prepared, filed, and served consistent with state law and the procedures developed by the substantial risk order coordinator (Va. Code § 19.2-152.13).

345.5 SERVICE OF ORDERS
Deputies shall serve a copy of a substantial risk order, along with any accompanying petition, supporting affidavit, notice of hearing, and other notices as applicable, on the person named in the order as soon as practicable (Va. Code § 19.2-152.13; Va. Code § 19.2-152.14).

Service of orders shall take precedence over the service of other orders, except for orders of a similar emergency nature (Va. Code § 19.2-152.13; Va. Code § 19.2-152.14).

345.5.1 PROOF OF SERVICE
Any member serving an emergency substantial risk order shall file with the court appropriate proof of service documents, which shall include an inventory of any firearms relinquished (Va. Code § 19.2-152.13; Va. Code § 19.2-152.14).

345.5.2 VIRGINIA CRIMINAL INFORMATION NETWORK
Any member assigned to address a substantial risk order received from the court (or its modification or dissolution) is required to verify that the appropriate information is entered into the Virginia Criminal Information Network as may be required by the Virginia State Police and as soon as practicable. If a court has already entered information regarding the order into the network, the information should still be verified and modified as necessary (Va. Code § 19.2-152.13; Va. Code § 19.2-152.14).

345.5.3 SAFETY CONSIDERATIONS
Upon receipt of a substantial risk order, the Operations Director or authorized designee should evaluate the circumstances of the order and consider what precautions are appropriate for service of the protection order.

When appropriate based on the circumstances and department procedures, service of an order should be executed pursuant to the Operations Planning and Deconfliction Policy.

In no circumstances should fewer than two deputies be present when an order is being served.

345.5.4 SURRENDER OF PROHIBITED ITEMS
Deputies serving a substantial risk order shall request that the named person immediately surrender all prohibited items as required by the order. Deputies shall take custody of any items surrendered pursuant to the order.

A receipt identifying all surrendered items shall be prepared by the deputies and a copy given to the person. Identifying information should include manufacturer, model, condition, and serial number of any firearm (Va. Code § 19.2-152.13). The deputies should ensure the original receipt is included in the original case report and forwarded to the Records Manager as soon as practicable.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

All items collected should be handled and booked in accordance with the Property and Evidence Section Policy.

345.5.5 SEARCH WARRANTS

Deputies should consider whether a search warrant may be reasonably necessary prior to attempting service of an order.

Deputies should also consider whether to seek a search warrant if the named person refuses to surrender any prohibited items or if a deputy serving a substantial risk order reasonably believes there are prohibited items within the person’s custody, control, or possession that have not been surrendered.

345.6 RELEASE OF PROHIBITED ITEMS

Any person requesting the release of any prohibited items in Department custody pursuant to a substantial risk order should be referred to the Property and Evidence Section.

345.7 RENEWAL OF A SUBSTANTIAL RISK ORDER

The Investigation Division supervisor is responsible for the review of any substantial risk order obtained by the Department to determine if renewal or extension of the order should be requested within the time prescribed by law (Va. Code § 19.2-152.14).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

School Resource Officers

346.1 PURPOSE AND SCOPE

This policy outlines the Madison County Sheriff's Office School Resource Officer (SRO) program.

346.2 POLICY

The Madison County Sheriff's Office is committed to enhancing the safety of students and faculty on campuses located in the department's jurisdiction by forming a partnership with school administrators, faculty members, and students.

346.3 SCHOOL RESOURCE OFFICER PROGRAM

The Sheriff shall appoint, in consultation with the school superintendent, at least one SRO to serve in public elementary and secondary schools. The goals and objectives of the SRO program partnership include but are not limited to:

(a) Creating respect for law and order in the public school system and minimizing criminal activity.

(b) Identifying students at risk of becoming involved in the criminal justice system and guiding them toward more positive and socially acceptable ways to behave.

(c) Reducing criminal activity on or near a school campus.

(d) Enhancing communication and understanding between students, their families, district staff, and the Department.

(e) Assisting with the coordination of security measures for school activities such as sports events, dances, and other large gatherings.

(f) Auditing security measures, at least annually, throughout the school and making recommendations to enhance safety and reduce risk.

The Sheriff shall enter into a memorandum of understanding (MOU) with the school superintendent concerning the deployment and responsibilities of SROs.

See attachment: MadiSon County School SRO MOU.pdf

346.4 SCHOOL RESOURCE OFFICER DUTIES

The Sheriff or the authorized designee should appoint members as SROs whose duties and responsibilities include:

(a) Responding to calls and conducting the preliminary investigation of criminal offenses that occur on student-occupied property while the SRO is on-duty or during school hours.

(b) Conducting follow-up investigations of misdemeanor offenses that occur on student-occupied property during school hours.

(c) Assisting the Investigations Division with follow-up investigations that originate on student-occupied property or involve a student.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Providing education for students, faculty, and administrators as requested and when available regarding law enforcement functions.

(e) Assisting faculty and administrators in establishing policies that contribute to the safety of school staff and students.

(f) Participating in student conferences, as requested and appropriate.

(g) Providing youth gang task force intelligence, as appropriate.

(h) Participating in the development of programs designed to identify, assess, and provide assistance to troubled youth.

(i) Assisting with the coordination of security measures for school activities such as sports events, dances, and other large gatherings.

(j) Assisting with the development and implementation of a school safety plan.

(k) Auditing security measures, at least annually, throughout the school and making recommendations to enhance safety and reduce risk.

346.4.1 CHAIN OF COMMAND

Selection, assignment, scheduling, training, supervision, and evaluation of SROs will be the responsibility of the Sheriff as informed by the input of school administrators and the identified needs and conditions of the schools. The SRO shall remain at all times under the control, through the chain of command, of the Sheriff.

Officers shall follow their assigned department chain of command during investigations of criminal activity. Assigned activities that are not criminal in nature may be overseen or directed by the school principal or the authorized designee or as otherwise provided in the MOU. SROs shall remain subject to the established policies and procedures of this Department at all times during the performance of their duties.

346.5 SCHOOL RESOURCE OFFICER QUALIFICATIONS

Members appointed as SROs shall be selected using criteria that includes but is not limited to):

(a) The ability of the appointee to foster an optimal learning environment and educational community.

(b) Demonstrated personality and character to work with children and educators in a school environment.

(c) Whether the candidate has specialized training in:

1. Child or adolescent cognitive development.
2. De-escalation and conflict resolution techniques with children and adolescents.
3. Behavioral health disorders in children and adolescents.
4. Alternatives to arrest and other juvenile justice diversion strategies.
5. Behavioral threat assessment methods.

(d) The ability to act as a mentor and positive role model for their student populations.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(e) Demonstrated commitment to de-escalation, diversion, and/or restorative justice, and an understanding of crime prevention, problem-solving, and community policing in a school setting.

The selection shall not be based solely on seniority. The performance of SROs shall be reviewed annually by the school district superintendent and the Sheriff or authorized designee.

346.6 SUPERVISION

The Sheriff shall appoint a Sergeant to act as the SRO Supervisor.The SRO Supervisor's responsibilities shall include:

(a) Acting as the liaison between the Office/Department and school administrative authorities concerning any operational or administrative issues that may arise

(b) Supervision including scheduling, training and evaluation of all assigned SROs.

(c) Responsibility to serve as a consultant for school safety and security issues including assessments and critical incident response planning.

(d) Maintain a working knowledge of school rules, regulations, and laws regarding student safety and conduct.

(e) Establishing and maintaining effective relationships with school personnel.

346.7 TRAINING

Within one year of their appointment as a School Resource Officer, officers shall complete a formal 40-hour SRO training program conducted or approved by the National Association of School Resource Officers or other similar school resource officer training sanctioned by the state police officer standards and training certification agency. The Sheriff should also ensure that SROs receive appropriate ongoing in-service joint training with their school administrators.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Chapter 4 - Patrol Operations

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Patrol

400.1 PURPOSE AND SCOPE

The purpose of this policy is to define the patrol function and address intraorganizational cooperation and information sharing.

400.2 POLICY

The Madison County Sheriff's Office provides patrol services 24 hours a day, seven days a week and will prioritize responses to requests for emergency services using available resources to enhance the safety of the public and department members.

400.3 FUNCTION

Patrol will generally be conducted by uniformed deputies in clearly marked law enforcement vehicles in assigned jurisdictional areas of Madison County, Virginia. The function of patrol is to respond to calls for assistance and reports of criminal activity, act as a deterrent to crime, enforce state and local laws, identify community needs, provide support and assistance to the community and respond to emergencies.

Patrol services include, but are not limited to:

(a) Responding to emergency calls for service.

(b) Apprehending criminal offenders.

(c) Providing mutual aid and assistance to other agencies for emergency and law enforcement-related activities.

(d) Preventing criminal acts, traffic violations and accidents, maintaining public order and discovering hazardous situations or conditions.

(e) Responding to reports of both criminal and non-criminal acts.

(f) Responding to routine calls for service, such as public assistance or public safety.

(g) Directing and controlling traffic.

(h) Carrying out crime prevention activities, such as residential inspections, business inspections and community presentations.

(i) Carrying out community-oriented policing and problem-solving activities, including the application of resources to improve or resolve specific problems or situations and contacting or assisting members of the public in a positive way.

(j) Providing courthouse/courtroom security, including operating physical security equipment, searching individuals and the facility, and developing high-risk trial plans and emergency evacuation plans, if applicable.

400.3.1 PATROL ASSIGNMENT

Patrol assignments should include a system that provides for:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) Assignment to operational shifts.

(b) Shift rotation, if any.

(c) Assignment to beats, if any.

(d) Beat rotation, if any.

(e) Continuous coverage during shift changes, if the Department operates on a shift schedule.

(f) Providing information to oncoming shifts of previous shifts' activities in accordance with the Briefing Policy.

400.4 INFORMATION SHARING

To the extent feasible, all information relevant to the mission of the Department should be shared among all divisions and specialized units on a timely basis. Members should be provided with opportunities on a regular basis to share information during the daily briefings and to attend briefings of other divisions or specialized units.

Additionally, information should be shared with outside agencies and the public in conformance with department policies and applicable laws. Members are encouraged to share information with other units and divisions.

400.5 CROWDS, EVENTS AND GATHERINGS

Deputies may encounter gatherings of people, including, but not limited to, civil demonstrations, public displays, parades, sporting events and civic, social and business events. Deputies should monitor such events as time permits in an effort to keep the peace and protect the safety and rights of those present. A patrol supervisor should be notified when it becomes reasonably foreseeable that such an event may require increased monitoring, contact or intervention.

Deputies responding to an event or gathering that warrants law enforcement involvement should carefully balance the speech and association rights of those present with applicable public safety concerns before taking enforcement action.

Generally, deputies should consider seeking compliance through advisements and warnings for minor violations, and should reserve greater enforcement options for more serious violations or when voluntary compliance with the law is not achieved.

Deputies are encouraged to contact organizers or responsible persons to seek voluntary compliance that may address relevant public safety concerns.

400.6 COMMUNITY-ORIENTED POLICING SERVICES

The Patrol Division Supervisor should ensure that a community-oriented policing program is established and includes at a minimum:

(a) The mission, organizational values and management principles that support community partnerships.

(b) A definition of community partnerships as a commitment to a philosophy rather than a program.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) A list of partnerships and collaborative efforts involving the Madison County Sheriff's Office and persons, groups and businesses within the community.

(d) Training for deputies and community leaders in the theory and concept, as well as function and operation, of community partnerships.

(e) Recommended training for members in problem-solving models.

(f) Materials that assist deputies in developing support from County officials for the concept of community-oriented policing, with the goal of County wide adoption of the community partnership philosophy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Bias-Based Policing

401.1 PURPOSE AND SCOPE

This policy provides guidance to department members that affirms the Madison County Sheriff's Office's commitment to policing that is fair and objective.

Nothing in this policy prohibits the use of specified characteristics in law enforcement activities designed to strengthen the department's relationship with its diverse communities (e.g., cultural and ethnicity awareness training, youth programs, community group outreach and partnerships).

401.1.1 DEFINITIONS

Definitions related to this policy include:

Bias-based policing - An inappropriate reliance on actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, disability, or affiliation with any non-criminal group (protected characteristics) as the basis for providing differing law enforcement service or enforcement. This includes any other noncriminal characteristics prohibited by state law (Va. Code § 15.2-1609.10; Va. Code § 15.2-1722.1; Va. Code § 52-30.1 et seq.).

401.2 POLICY

The Madison County Sheriff's Office is committed to providing law enforcement services to the community with due regard for the racial, cultural or other differences of those served. It is the policy of this department to provide law enforcement services and to enforce the law equally, fairly, objectively and without discrimination toward any individual or group.

401.3 BIAS-BASED POLICING PROHIBITED

Bias-based policing is strictly prohibited.

However, nothing in this policy is intended to prohibit a deputy from considering protected characteristics in combination with credible, timely and distinct information connecting a person or people of a specific characteristic to a specific unlawful incident, or to specific unlawful incidents, specific criminal patterns or specific schemes.

401.4 MEMBER RESPONSIBILITIES

Every member of this department shall perform his/her duties in a fair and objective manner and is responsible for promptly reporting any suspected or known instances of bias-based policing to a supervisor. Members should, when reasonable to do so, intervene to prevent any bias-based actions by another member.

401.4.1 REASON FOR CONTACT

Deputies contacting a person shall be prepared to articulate sufficient reason for the contact, independent of the protected characteristics of the individual.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

To the extent that written documentation would otherwise be completed (e.g., arrest report, field interview (FI) card), the involved deputy should include those facts giving rise to the contact, as applicable.

Except for required data-collection forms or methods, nothing in this policy shall require any deputy to document a contact that would not otherwise require reporting.

401.4.2 REPORTING TRAFFIC STOPS

Each time a deputy makes a traffic stop, stops and frisks a person based on reasonable suspicion, or temporarily detains a person during any other investigatory stop, the deputy shall record the following information on the appropriate forms provided by the Department (Va. Code § 52-30.2; Va. Code § 52-30.4; 19 VAC 30-240-10):

(a) The race, ethnicity, age, and gender of the person

(b) Whether the person spoke English

(c) The reason for the stop, as well as its location and the outcome

(d) Whether any search was made

(e) Whether the deputy used physical force against any person and whether any person used physical force against any deputies

(f) Any other information noted on the designated form

The Patrol Division Supervisor or the authorized designee should establish procedures as necessary for the department's compliance with Va. Code § 52-30.2 and Va. Code § 52-30.4; 19 VAC 30-240-10.

401.5 SUPERVISOR RESPONSIBILITIES

Supervisors should monitor those individuals under their command for compliance with this policy and shall handle any alleged or observed violations in accordance with the Personnel Complaints Policy.

(a) Supervisors should discuss any issues with the involved deputy and his/her supervisor in a timely manner.

    1. Supervisors should document these discussions, in the prescribed manner.

(b) Supervisors should periodically review Mobile Audio/Video (MAV) recordings, portable audio/video recordings, Mobile Data Computer (MDT) data and any other available resource used to document contact between deputies and the public to ensure compliance with this policy.

    1. Supervisors should document these periodic reviews.

    2. Recordings or data that capture a potential instance of bias-based policing should be appropriately retained for administrative investigation purposes.

(c) Supervisors shall initiate investigations of any actual or alleged violations of this policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Supervisors should take prompt and reasonable steps to address any retaliatory action taken against any member of this department who discloses information concerning bias-based policing.

401.6 STATE REPORTING

The Sheriff or the authorized designee shall collect the information required by law relating to use of excessive force complaints, traffic stops, and other detentions, and shall report that information to the Department of State Police and publish it in the manner provided by law (Va. Code § 15.2-1609.10; Va. Code § 15.2-1722.1; Va. Code § 52-30.2; Va. Code § 52-30.4; 19 VAC 30-240-10; 19 VAC 30-240-20).

All complaints regarding bias-based profiling, including those investigated by a member's immediate supervisor, shall be forwarded to the Internal Affairs Unit for any additional required investigation or disposition.

401.7 ADMINISTRATION

The Patrol Division Supervisor should review the efforts of the Department to provide fair and objective policing and submit an annual report, including public concerns and complaints, to the Sheriff. The annual report should not contain any identifying information about any specific complaint, member of the public, or deputy. It should be reviewed by the Sheriff to identify any changes in training or operations that should be made to improve service.

Supervisors should review the traffic stop data, use of excessive force complaint data, and the annual report and discuss the results with those they are assigned to supervise.

401.8 TRAINING

Training on fair and objective policing and review of this policy should be conducted as directed by the Training Supervisor.

401.8.1 INITIAL TRAINING

Newly hired deputies shall receive initial training in cultural diversity.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Briefing

402.1 PURPOSE AND SCOPE

This policy discusses the activity of briefing and includes the tasks that should be accomplished during this short period.

402.2 POLICY

Briefing is intended to facilitate the accurate flow of information in order to enhance coordination of activities, improve performance and safety, and outline the expected actions of members.

402.3 BRIEFING

All divisions and specialized units will conduct regular briefing to discuss, disseminate and exchange information among department members, work groups and other organizations. A supervisor generally will conduct briefing. However, the supervisor may delegate this responsibility to a subordinate member in his/her absence or for training purposes.

Briefing should include, but is not limited to:

(a) Providing members with information regarding daily activities, with particular attention given to changes in the status of:
    1. Wanted persons.
    2. Crime patterns.
    3. Suspect descriptions.
    4. Intelligence reports and photographs.
    5. Community issues affecting law enforcement.
    6. Major investigations.

(b) Notifying members of changes in schedules and assignments.

(c) Reviewing recent incidents for situational awareness and training purposes.

(d) Providing training on a variety of subjects.

(e) Conducting periodic personnel inspections.

Supervisors should also ensure that all members are informed about General Orders and any recent policy changes.

402.3.1 RETENTION OF BRIEFING TRAINING RECORDS

Briefing training materials and a curriculum or summary shall be forwarded to the Training Supervisor for inclusion in training records, as appropriate.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Briefing

402.4 PREPARATION OF MATERIALS

The member conducting briefing is responsible for preparation of the materials necessary for a constructive briefing.

402.5 TRAINING

Briefing training should incorporate short segments on a variety of subjects or topics and may include:

(a) Review and discussion of new or updated policies.

(b) Presentation and discussion of the proper application of existing policy to routine daily activities.

(c) Presentation and discussion of the proper application of existing policy to unusual activities.

(d) Review of recent incidents for training purposes.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Crime and Disaster Scene Integrity

403.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance in handling a major crime or disaster.

403.2 POLICY

It is the policy of the Madison County Sheriff's Office to secure crime or disaster scenes so that evidence is preserved, and to identify and mitigate the dangers associated with a major crime or disaster scene for the safety of the community and those required to enter or work near the scene.

403.3 SCENE RESPONSIBILITY

The first deputy at the scene of a crime or major incident is generally responsible for the immediate safety of the public and preservation of the scene. Deputies shall also consider officer safety and the safety of those persons entering or exiting the area, including those rendering medical aid to any injured parties. Once a deputy has assumed or been assigned to maintain the integrity and security of the crime or disaster scene, it shall be maintained until the deputy is properly relieved by a supervisor or other designated person.

403.4 FIRST RESPONDER CONSIDERATIONS

The following list generally describes the first responder’s function at a crime or disaster scene. This list is not intended to be all-inclusive, is not necessarily in order and may be altered according to the demands of each situation:

(a) Broadcast emergency information, including requests for additional assistance and resources.

(b) Provide for the general safety of those within the immediate area by mitigating, reducing or eliminating threats or dangers.

(c) Locate or identify suspects and determine whether dangerous suspects are still within the area.

(d) Provide first aid to injured parties if it can be done safely.

(e) Evacuate the location safely as required or appropriate.

(f) Secure the inner perimeter.

(g) Protect items of apparent evidentiary value.

(h) Secure an outer perimeter.

(i) Identify potential witnesses.

(j) Start a chronological log noting critical times and personnel allowed access.

403.5 SEARCHES

Deputies arriving at crime or disaster scenes are often faced with the immediate need to search for and render aid to victims, and to determine if suspects are present and continue to pose a threat.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Once deputies are satisfied that no additional suspects are present and/or there are no injured persons to be treated, those exigent circumstances will likely no longer exist. Deputies should thereafter secure the scene and conduct no further search until additional or alternate authority for the search is obtained, such as consent or a search warrant.

403.5.1 CONSENT

When possible, deputies should seek written consent to search from authorized individuals. However, in the case of serious crimes or major investigations, it may be prudent to also obtain a search warrant. Consent as an additional authorization may be sought, even in cases where a search warrant has been granted.

403.6 INVESTIGATION DIVISION SUPERVISOR RESPONSIBILITIES

The Investigation Division Supervisor is responsible for:

(a) Ensuring reasonable access to qualified personnel, equipment and supplies for processing crime scenes.

(b) Establishing procedures for collecting, processing and preserving physical evidence in the field.

(c) Establishing procedures for photographing, video-recording and other imaging used to collect and preserve evidence.

(d) Establishing procedures for processing, developing, lifting and labeling fingerprints.

(e) Establishing procedures for the safe collection, storage, transportation and submission of biological and other evidence for DNA testing and evaluation.

403.7 EXECUTION OF HEALTH ORDERS

Any sworn member of this department is authorized to enforce lawful orders of the local health officer that have been issued for the purpose of preventing the spread of any contagious, infectious or communicable disease (Va. Code § 32.1-48.02).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Crisis Response Unit

404.1 PURPOSE AND SCOPE

This policy provides guidelines for the specialized support of the Crisis Response Unit (CRU) in handling critical field operations where special tactical deployment methods or intense negotiations are beyond the capacity of field deputies. Where circumstances dictate a level of manpower and resources beyond that which is available internally, the Sheriff's Department will request assistance from the Virginia State Police Tactical Team.

404.1.1 DEFINITIONS

Definitions related to this policy include:

Negotiation team - Designated deputies, including those in a multijurisdictional team, who are specifically trained and equipped to provide skilled verbal communications to de-escalate or effect surrender in situations where suspects have taken hostages or barricaded themselves or are suicidal.

Tactical team - Designated deputies, including those in a multijurisdictional team, who are specifically trained and equipped to resolve critical incidents that are so hazardous, complex or unusual that they may exceed the capabilities of first responders or investigators. This includes, but is not limited to, hostage taking, barricaded suspects, snipers, terrorist acts and other high-risk incidents. As a matter of department policy, a tactical team may also be used to serve high-risk warrants, both search and arrest, where public and officer-safety issues necessitate such use.

404.2 POLICY

It shall be the policy of the Madison County Sheriff's Office to maintain a CRU, either internally or through participation in a regional team, comprised of negotiation and tactical teams, and to provide the equipment, manpower and training necessary to maintain such teams. The CRU should develop sufficient resources to perform three basic operational functions:

(a) Command and control

(b) Containment

(c) Entry/apprehension/rescue

404.3 CAPABILITIES

This department acknowledges that training needs may vary based on the experience level of team members, team administrators and potential incident commanders. Therefore, with the preservation of innocent human life being paramount, nothing in this policy shall prohibit individual teams from responding to a situation that exceeds their training level due to the exigency of the circumstances.

The various levels of tactical team capability and training are as follows and may fluctuate based upon personnel, training, available equipment, resources and capabilities:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

- Level I - A basic team capable of providing containment and intervention in critical incidents that exceed the training and resources available to line-level deputies. This does not include ad hoc teams of deputies that are formed around a specific mission, detail or incident (e.g., active shooter response). Generally 5 percent of the Level I team's on-duty time should be devoted to training.
- Level II - An intermediate-level tactical team capable of providing containment and intervention. These teams possess tactical capabilities above the Level I teams. These teams may or may not work together on a daily basis, but are intended to respond to incidents as a team. At least 5 percent of the Level II team's on-duty time should be devoted to training with supplemental training for tactical capabilities above the Level I team.
- Level III - An advanced-level tactical team whose members function on a full-time basis. Generally 25 percent of the Level III team's on-duty time is devoted to training. Level III teams operate in accordance with contemporary best practices. Such teams possess both skills and equipment to utilize tactics beyond the capabilities of Level I and Level II teams.

The Madison County Sheriff's Department will field a Level I Crisis Response Unit (CRU).

404.4 MANAGEMENT AND SUPERVISION

Under the direction of the Sheriff, through the Patrol Division Captain, the CRU shall be managed by the appointed CRU Commander. The CRU Commander shall be selected by the Sheriff upon recommendation of command staff.

404.4.1 TEAM SUPERVISORS

The negotiation team and tactical team will be under the direction of designated team supervisors, who shall be selected by the Sheriff upon specific recommendation by command staff and the CRU Commander.

The primary responsibility of the team supervisors is to oversee the operation of their teams, which includes deployment, training, first-line supervisor participation and other duties as directed by the CRU Commander.

404.5 READINESS

An operational readiness assessment should be conducted to determine the type and extent of CRU missions and operations appropriate to this department. The assessment should consider the capabilities, training and limitations of the CRU and should be reviewed annually by the CRU Commander or the authorized designee.

404.5.1 EQUIPMENT INSPECTIONS

The CRU Commander shall appoint a team supervisor to perform operational readiness inspections of all CRU equipment at least quarterly. The result of the inspection will be forwarded to the CRU Commander in writing. The inspections will include personal equipment issued to members of the CRU, operational equipment maintained in the CRU facility and equipment maintained or used in CRU vehicles.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

404.5.2 MULTIJURISDICTIONAL OPERATIONS

The CRU, including any relevant specialized teams and supporting resources, should develop protocols, agreements, memorandums of understanding (MOUs) or working relationships to support multijurisdictional or regional responses.

(a) If it is anticipated that multijurisdictional CRU operations will regularly be conducted, multi-agency and multidisciplinary joint training exercises should occur.

(b) Members of the Madison County Sheriff's Office CRU shall operate under the policies, procedures and command of the Madison County Sheriff's Office when working in a multi-agency situation.

404.6 PROCEDURES

Situations that necessitate the need for a CRU response vary greatly from incident to incident and often demand on-scene evaluation. The guidelines allow for appropriate on-scene decision-making and development of organizational and operational procedures.

404.6.1 ORGANIZATIONAL PROCEDURES

The Department shall develop a separate written set of organizational procedures that should address, at a minimum:

(a) Specific missions the CRU is capable of performing.

(b) CRU organization and function.

(c) Member selection, retention and termination criteria.

(d) Training and required competencies, including record production and retention.

(e) Procedures for notification, activation, deactivation and deployment.

(f) Command and control issues, including a clearly defined command structure and dedicated lines of communication.

(g) Multi-agency response.

(h) Out-of-jurisdiction response.

(i) Specialized functions and supporting resources.

404.6.2 OPERATIONAL PROCEDURES

The Department shall develop a separate written set of operational procedures in accordance with the determination of the CRU's level of capability, using sound risk-reduction practices. The operational procedures should be patterned after the National Tactical Officers Association's (NTOA) SWAT Standard for Law Enforcement Agencies. Because such procedures are specific to CRU members and outline negotiation, tactical and officer-safety issues, they are not included within this policy.

The operational procedures should include, at a minimum:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Crisis Response Unit

(a) Designation of members who are responsible for developing an operational or tactical plan prior to, and/or during CRU operations (time permitting).

1. All CRU members should have an understanding of operational planning.
2. CRU training should include planning for both spontaneous and planned events.
3. CRU planning should incorporate medical emergency contingency plans as part of the CRU operational plan.

(b) Plans for mission briefings conducted prior to an operation, unless circumstances require immediate deployment.

1. When possible, briefings should include the specialized teams, certified tactical dispatchers and other supporting personnel.

(c) Protocols for a sustained operation to be developed that may include relief, rotation of members and augmentation of personnel and resources.

(d) A generic checklist to be worked through prior to initiating a tactical action as a means of conducting a threat assessment to determine the appropriate response and resources necessary, including the use of the CRU.

(e) Roles for the negotiations team and negotiators.

(f) A standard method of determining whether a warrant should be regarded as high risk.

(g) A method for deciding how best to serve a high-risk warrant with all reasonably foreseeable alternatives being reviewed in accordance with risk/benefit criteria prior to selecting the method of response.

(h) Protocols for post-incident scene management, including:

1. Documentation of the incident.
2. Transition to investigations and/or other divisions.
3. Debriefing after every deployment of the CRU.
    (a) After-action team debriefing provides evaluation and analysis of critical incidents, affords the opportunity for individual and team assessments, helps to identify training needs and reinforces sound risk management practices.
    (b) Such debriefing should not be conducted until involved members have had the opportunity to individually complete necessary reports or provide formal statements.
    (c) In order to maintain candor and a meaningful exchange, debriefing will generally not be recorded.
    (d) When appropriate, debriefing should include specialized teams and supporting or assisting personnel.

(i) A sound risk management analysis.

(j) Standardization of equipment deployed.

See attachment: Threat Assessment Matrix.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

404.7 OPERATIONAL GUIDELINES

The following are guidelines for the operational deployment of the CRU. Generally, the tactical team and the negotiation team will be activated together. It is recognized, however, that the teams can be activated independently as circumstances dictate. The tactical team may be used in a situation not requiring the physical presence of the negotiation team, such as warrant service operations. The negotiation team may be used in a situation not requiring the physical presence of the tactical team, such as handling a suicidal person. Operational deployment of the specialized teams shall be at the discretion of the Sheriff or, if the Sheriff is not available, the Crisis Response Unit Commander.

404.7.1 APPROPRIATE USE

Incidents that may result in the activation of the CRU include:

(a) Barricaded suspects who refuse an order to surrender.

(b) Incidents where hostages are taken (Notify Virginia State Police Tactical Team).

(c) Individuals who are threatening suicide and have refused to surrender.

(d) Arrests of potentially armed or dangerous persons.

(e) Any situation that could threaten or undermine the ability of the Department to preserve life, maintain social order and ensure the protection of persons or property.

Requests by field personnel for assistance from crisis response units from another agency must be approved by the Sheriff. Deployment of the Madison County Sheriff's Office CRU in response to requests by other agencies must be authorized by the Sheriff.

404.7.2 ON-SCENE DETERMINATION AND NOTIFICATION

The supervisor-in-charge at the scene of a particular event will be designated as the Incident Commander and will contact the Sheriff and the CRU Commander to respond to the scene. If the CRU Commander is unavailable, then a specialized team supervisor shall be notified.

NOTE: Upon determination that the incident involves s suspect who is in control of hostages and barricaded the Sheriff will notify the Virginia State Police Tactical Team.

The Shift Supervisor should brief the CRU Commander about the incident. Such information should include:

(a) The type of crime involved.

(b) The number of suspects, identity and criminal history.

(c) The known weapons and resources available to the suspect.

(d) If the suspect is in control of hostages and/or barricaded.

(e) Whether contact has been made with the suspect and whether there have been demands.

(f) If potential victims are still within the inner perimeter.

(g) If the suspect has threatened or attempted suicide.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(h) The location of the command post and a safe approach to it.

(i) The extent of any inner or outer perimeter and the number of personnel involved.

(j) Any other assets or resources at the scene including other involved agencies.

(k) Whether the situation meets the criteria of the Threat Assessment Matrix for CRU callout.

(l) Any other important facts critical to the immediate situation.

The CRU Commander or team supervisor shall then follow current callout procedures. A current mobilization list shall be maintained in the Shift Supervisor's office and the Dispatch Center by the CRU Commander.

The Shift Supervisor will notify the Patrol Division Supervisor as soon as practicable.

404.7.3 FIELD PERSONNEL RESPONSIBILITIES

While waiting for the CRU to respond, field personnel should, if determined to be safe and practicable and sufficient resources exist:

(a) Establish an arrest/response team in case the suspect takes action. The response team's tasks may include:

1. Taking action to mitigate a deadly threat or behavior either inside or outside the location.
2. Securing any subject or suspect who may surrender or attempt to escape.

(b) Evacuate any injured persons in the zone of danger.

(c) Evacuate or provide safety instructions to other people in the zone of danger.

(d) Establish an inner and outer perimeter.

(e) Establish a command post outside of the inner perimeter in a secure location.

(f) Attempt to establish preliminary communication with the suspect. Once the CRU has arrived, all negotiations should generally be halted to allow the negotiation and tactical teams time to organize, position and assume the appropriate roles and responsibilities.

(g) Plan for, and stage, anticipated resources.

404.7.4 ON-SCENE COMMAND RESPONSIBILITIES

Upon arrival of the CRU at the scene, the Shift Supervisor shall brief the CRU Commander and team supervisors. Upon review, it will be the CRU Commander's decision as to whether to deploy the CRU. Once the CRU Commander authorizes deployment, the CRU Commander or the authorized designee will be responsible for the tactical response and negotiations. The Incident Commander shall continue to supervise the command post operation, outer perimeter security, evacuation and media access and will support the CRU. The Incident Commander and CRU Commander or the authorized designee shall maintain direct communication at all times.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

404.7.5 COMMUNICATIONS WITH CRU MEMBERS

All persons who are non-CRU members should refrain from any non-emergency contact or interference with any CRU member during active negotiations. CRU operations require the utmost in concentration by involved members and, as a result, no one should interrupt or communicate with CRU members directly. All non-emergency communications shall be channeled through the negotiation team or tactical team supervisor or the authorized designee.

404.8 TACTICAL TEAM ADMINISTRATIVE GUIDELINES

The tactical team was established to provide a skilled and trained team for deployment to events that require specialized tactics, in situations where suspects have taken hostages and/or barricaded themselves, and in prolonged or predictable situations where persons who are armed or suspected of being armed pose a danger to themselves or others.

The following procedures serve as directives for the administrative operation of the tactical team.

404.8.1 SELECTION OF TACTICAL MEMBERS

Interested CRU members who are off probation shall submit a change of assignment request to their appropriate Division Supervisors, a copy of which will be forwarded to the CRU Commander and other tactical team supervisors. Those qualifying applicants will then be invited to participate in the testing process. The order of the tests will be at the discretion of the CRU Commander. The testing process will consist of an oral interview, physical agility test, firearm qualification and team evaluation.

(a) Oral interview: The oral interview will be conducted by individuals selected by the CRU Commander. Applicants will be evaluated by certain criteria, which includes:

1. Recognized competence and ability, as evidenced by performance.
2. Demonstrated good judgment and understanding of the critical role of a tactical team member.
3. Special skills, training or appropriate education as it pertains to this assignment.
4. Commitment to the CRU, realizing that the additional assignment may necessitate unusual working hours, conditions and training obligations.

(b) Physical agility: The physical agility test is designed to determine the physical capabilities of the applicant as they relate to performance of tactical team-related duties. The test and scoring procedure will be established by the CRU Commander. A minimum qualifying score shall be attained by the applicant to be considered for the position.

(c) Firearm qualification: Candidates will be invited to shoot the CRU basic drill for the handgun. A minimum qualifying score established by the Rangemaster must be attained to qualify.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Team evaluation: Current team members will evaluate each candidate on field tactical skills, teamwork, ability to work under stress, communication skills, judgment and any special skills that could benefit the team.

The CRU Commander shall submit a list of successful applicants to command staff for final selection.

404.8.2 TACTICAL TRAINING

Training shall be coordinated by the CRU Commander. The CRU Commander may conduct monthly training exercises that include a review and critique of members and their performance in the exercises, in addition to specialized training. Training shall consist of the following:

(a) Each tactical team member shall perform a physical fitness test annually. A minimum qualifying score must be attained by each team member.

(b) Any tactical team member failing to attain the minimum physical fitness qualification score will be notified of the requirement to retest. Within 30 days of the previous physical fitness test date, the member required to qualify shall report to a team supervisor and complete the entire physical fitness test. Failure to qualify after a second attempt may result in dismissal from the team.

(c) Those who are on vacation, are ill or are on light-duty status with a medical professional's note of approval on the test date shall be responsible for reporting to a team supervisor and taking the test within 30 days of their return to regular duty. Any member who fails to arrange for and perform the physical fitness test within the 30-day period shall be considered as having failed to attain a qualifying score for that test period.

(d) Each tactical team member shall complete the quarterly tactical team handgun qualification course. The qualification course shall consist of the CRU basic drill for the handgun. Failure to qualify will require the team member to seek remedial training from a Rangemaster who has been approved by the CRU Commander. Team members who fail to qualify will not be used in CRU operations until qualified. Team members who fail to qualify must retest within 30 days. Failure to qualify within 30 days, with or without remedial training, may result in dismissal from the team.

(e) Each tactical team member shall complete the quarterly tactical qualification course for any specialty weapon issued to, or used by, the team member during tactical team operations. Failure to qualify will require the team member to seek remedial training from a Rangemaster who has been approved by the CRU Commander. Team members who fail to qualify on their specialty weapon may not utilize the specialty weapon on CRU operations until qualified. Team members who fail to qualify must retest within 30 days. Failure to qualify with specialty weapons within 30 days may result in the team member being removed from the team or permanently disqualified from use of that particular specialty weapon.

404.8.3 TACTICAL TEAM EVALUATION

Continual evaluation of a team member’s performance and efficiency as it relates to the positive operation of the team shall be conducted by the team supervisor. The performance and efficiency

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

level, as established by the team supervisor, will be met and maintained by all tactical team members. Any member of the tactical team who performs or functions at a level less than satisfactory shall be subject to dismissal from the team.

404.9 NEGOTIATION TEAM ADMINISTRATIVE GUIDELINES

The negotiation team has been established to provide skilled verbal communicators who will attempt to de-escalate and effect surrender in critical situations where suspects have taken hostages or barricaded themselves or have suicidal tendencies.

The following procedures serve as directives for the administrative operation of the negotiation team.

404.9.1 SELECTION OF NEGOTIATION MEMBERS

Interested department members who are off probation shall submit a change of assignment request to their appropriate Division Supervisors. A copy will be forwarded to the CRU Commander and the negotiation team supervisor. Qualified applicants will then be invited to an oral interview. The oral interview board will consist of the CRU Commander, the negotiation team supervisor and a third person to be selected by the two. Interested members shall be evaluated by certain criteria, which include:

(a) Recognized competence and ability as evidenced by performance.

(b) Demonstrated good judgment and understanding of the critical role of a negotiator and the negotiation process.

(c) Effective communication skills.

(d) Special skills, training or appropriate education as it pertains to the assignment.

(e) Commitment to the CRU, realizing that the assignment may necessitate unusual working hours, conditions and training obligations.

The oral interview board shall submit a list of successful applicants to command staff for final selection.

404.9.2 NEGOTIATION TRAINING

Training shall be coordinated by the CRU Commander. The CRU Commander may conduct monthly training exercises that include a review and critique of members and their performance in the exercises, in addition to specialized training.

A minimum of one training day per quarter will be required to provide the opportunity for role playing and situational training necessary to maintain proper skills. This will be coordinated by the team supervisor.

404.9.3 NEGOTIATION TEAM EVALUATION

Continual evaluation of a team member's performance and efficiency as it relates to the positive operation of the team shall be conducted by the team supervisor. Performance and efficiency levels, established by the team supervisor, will be met and maintained by all team members. Any

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

member of the negotiation team who performs or functions at a level less than satisfactory shall be subject to dismissal from the team.

404.10 UNIFORMS AND EQUIPMENT

CRU specialized teams from this department should wear uniforms that clearly identify them as law enforcement members. It is recognized that certain tactical conditions may require covert movement. Attire may be selected that is appropriate to the specific mission.

404.10.1 EQUIPMENT

CRU specialized teams from this department should be adequately equipped to meet the specific missions identified by the Department.

404.10.2 FIREARMS

Weapons and equipment used by the CRU specialized teams and any supporting resources should be department-issued or approved, including any modifications, additions or attachments.

404.11 TRAINING

The CRU Commander shall conduct an annual CRU training needs assessment to ensure that training correlates to the team's capabilities and department policy.

404.11.1 TRAINING SAFETY

Use of a designated safety officer should be considered for all tactical training.

404.11.2 INITIAL TRAINING

Tactical and negotiation team members and team supervisors should not be deployed until successful completion of a basic CRU course or its equivalent that has been approved by this department.

(a) To avoid unnecessary or redundant training, previous training completed by members may be considered equivalent when the hours and content or topics meet or exceed requirements determined by the Department.

(b) Untrained members may be used in a support or training capacity.

404.11.3 UPDATE/REFRESHER TRAINING

Tactical and negotiation team members, team supervisors and certified tactical dispatchers should complete update or refresher training every 24 months.

404.11.4 MANAGEMENT TRAINING

Command and executive personnel are encouraged to attend training for managing the CRU functions at the organizational level. This is to ensure that those who provide active oversight at the scene understand the purpose and capabilities of these specialized teams.

Command personnel who may assume incident command responsibilities should attend a tactical commander or critical incident commander course or its equivalent that has been approved by this department.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

404.11.5 SCENARIO-BASED TRAINING

CRU specialized teams should participate in scenario-based training that simulates the critical field operations environment. Such training is an established method of improving performance during an actual deployment.

404.11.6 TRAINING DOCUMENTATION

Individual and team training shall be documented and records maintained by the Training Supervisor. Such documentation shall be maintained in each member’s training file. A separate department CRU training file shall be maintained with documentation and records of all team training.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Ride-Alongs

405.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for a ride-along with members of the Madison County Sheriff's Office. This policy provides the requirements, approval process, hours of operation and member responsibilities for ride-alongs.

405.2 POLICY

Ride-along opportunities will be provided to the members of the public, County employees and members of this department to observe and experience, first-hand, various functions of the Madison County Sheriff's Office. The term “ride-along” includes riding as a passenger with a deputy on patrol or observing the work day of members engaged in other functions within the Department, such as the Dispatch Center.

405.3 ELIGIBILITY

A ride-along is available to Madison County, Virginia residents and business owners, students currently attending class in Madison County, Virginia and those employed within the County of Madison County, Virginia. Efforts will be made to accommodate all interested persons. However, any applicant may be disqualified without cause from participating.

Factors that may be considered in disqualifying an applicant include, but are not limited to:

- Being under 15 years of age.
- Prior criminal history.
- Pending criminal action.
- Pending lawsuit against this department or the County.
- Denial by any supervisor.

405.4 AVAILABILITY

A ride-along or job observation is available most days of the week, from 10:00 a.m. to 11:00 p.m. Exceptions to this schedule may be made as approved by the Sheriff or Shift Supervisor.

405.5 REQUESTS TO PARTICIPATE

Generally, ride-along and job observation requests will be maintained and scheduled by the Shift Supervisor. The applicant will complete and sign a ride-along or job observation waiver form. If the applicant is under 18 years of age, a parent or guardian must be present to complete the waiver form. Information requested will include a valid state-issued identification card or driver's license number, birthdate, address and telephone number.

The Shift Supervisor will schedule a date, based on availability, generally one week after the date of application. If approved, a copy of the waiver form will be forwarded to the appropriate division as soon as possible for scheduling considerations.

If the request is denied, a representative of this department will advise the applicant of the denial.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

See attachment: Ride-Along Application and Liability Waiver.pdf

405.6 PROCEDURES

Once approved, ride-along applicants will be allowed to participate no more than once every six months. An exception may apply to the following law enforcement-involved participants:

- Explorers
- Volunteers
- Chaplains
- Auxiliaries
- Madison County Sheriff's Office applicants
- Any others with approval of the Shift Supervisor
- Students enrolled in any department-approved dispatcher training course

An effort will be made to ensure that no more than one member of the public will participate in a ride-along or job observation during any given time period. Normally, no more than one ride-along participant will be allowed in department vehicles at a given time.

Ride-along requirements for department Explorers are covered in the Explorers Policy.

405.6.1 OFF-DUTY PARTICIPATION

Off-duty members of this department or any other law enforcement agency, and employees of the County, will not be permitted to participate in a ride-along with on-duty members of this department without the express consent of the Shift Supervisor.

In the event that such participation is permitted, the off-duty department member, other law enforcement agency personnel or County employee shall not:

(a) Be considered on-duty.

(b) Represent him/herself as a member of this department or any other law enforcement agency.

(c) Participate in any law enforcement activity except as emergency circumstances may require.

405.6.2 CRIMINAL HISTORY CHECK

All ride-along applicants are subject to a criminal history check. The criminal history check may include a local records check and a Virginia Criminal Justice Information Services (CJIS) check prior to approval of the ride-along.

405.6.3 SUITABLE ATTIRE

Any person approved to participate in a ride-along is required to be suitably dressed in a collared shirt, blouse or jacket, slacks and shoes. Sandals, t-shirts, tank tops, shorts and ripped or torn pants are not permitted. Hats and ball caps will not be worn without the express consent of the

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Shift Supervisor. The Shift Supervisor or a supervisor may refuse a ride-along to anyone who is not dressed appropriately.

405.7 MEMBER RESPONSIBILITIES

The assigned department member shall consider the safety of the ride-along or job observation participant at all times. The member shall maintain control over the participant and shall instruct the individual about the conditions that necessarily limit his/her participation. Instructions should include:

(a) The participant will follow the directions of the department member.

(b) The participant will not become involved in any investigation, handling of evidence, discussions with victims or suspects, reading an individual's criminal history or other protected information, or handling any sheriff's department equipment.

(c) Participation may be terminated at any time by the member if the participant interferes with the performance of the member's duties.

    1. If the ride-along is in progress, the member may return the participant to the point the ride originated.

(d) Participants may be allowed to continue a ride-along during the transportation and booking process, provided it does not jeopardize their safety.

(e) Members will not allow participants to be present in any location or situation that would jeopardize the participant's safety or cause undue stress or embarrassment to a victim or any other member of the public.

(f) Participants who are not law enforcement officers shall not be permitted to accompany the department member into a private residence without the express consent of the resident or other authorized person.

The member assigned to provide a ride-along shall advise the dispatcher that a ride-along participant is present in the vehicle before going into service. A deputy with a ride-along participant should use sound discretion when encountering a potentially dangerous situation, such as a high-speed pursuit and, if feasible, let the participant out of the vehicle in a well-lit public place. The dispatcher will be advised of the situation and as soon as practicable have another department member respond to pick up the participant at that location. The ride-along may be continued or terminated at this time.

Conduct by a person participating in a ride-along that results in termination of the ride, or is otherwise inappropriate, should be immediately reported to the Shift Supervisor. The member should enter comments regarding the reasons for terminating the ride-along on the waiver form.

Upon completion of the ride-along, the member shall return the waiver form to the Shift Supervisor.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Hazardous Material Response

406.1 PURPOSE AND SCOPE

Exposure to hazardous materials presents potential harm to department members and the public. This policy outlines the responsibilities of members who respond to these events and the factors that should be considered while on-scene, including the reporting of exposures and supervisor responsibilities.

406.1.1 DEFINITIONS

Definitions related to this policy include:

Hazardous material - A substance which, by its nature, containment or reactivity, has the capability of inflicting harm during exposure; characterized as being toxic, corrosive, flammable, reactive, an irritant or strong sensitizer and thereby posing a threat to health when improperly managed.

406.2 POLICY

It is the policy of the Madison County Sheriff's Office to respond to hazardous material emergencies with due regard for the safety of the public and those members responding to such incidents.

406.3 HAZARDOUS MATERIAL RESPONSE

Members may encounter situations involving suspected hazardous materials, such as at the scene of a traffic accident, chemical spill or fire. When members come into contact with a suspected hazardous material, they should take certain steps to protect themselves and other persons.

The fire department is the agency trained and equipped to properly respond to and mitigate most incidents involving hazardous materials and biohazards.

Responders should not perform tasks or use equipment without proper training. A responder entering the area may require decontamination before he/she is allowed to leave the scene, and should be evaluated by appropriate technicians and emergency medical services personnel for signs of exposure.

406.4 CONSIDERATIONS

The following steps should be considered at any scene involving suspected hazardous materials:

(a) Make the initial assessment of potentially hazardous material from a safe distance.

(b) Notify the Dispatch Center, appropriate supervisors, the appropriate fire department, and hazardous response units.

1. Provide weather conditions, wind direction, a suggested safe approach route, and any other information pertinent to responder safety.

(c) Wear personal protective gear, being cognizant that some hazardous material can be inhaled.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Remain upwind, uphill, and at a safe distance, maintaining awareness of weather and environmental conditions, until the material is identified and a process for handling has been determined.

(e) Attempt to identify the type of hazardous material from a safe distance using optical aids (binoculars or spotting scopes) if they are available. Identification can be determined by:

1. Placards or use of an emergency response guidebook.
2. Driver's statements or shipping documents from the person transporting the material.
3. Information obtained from any involved person with knowledge regarding the hazardous material. Information should include:
    (a) The type of material.
    (b) How to secure and contain the material.
    (c) Any other information to protect the safety of those present, the community and the environment.

(f) Provide first aid to injured parties if it can be done safely and without contamination.

(g) Make reasonable efforts to secure the scene to prevent access from unauthorized individuals and to protect and identify any evidence.

(h) Begin evacuation of the immediate and surrounding areas, dependent on the material. Voluntary evacuation should be considered; mandatory evacuation may be necessary and will depend on the type of material.

(i) Establish a decontamination area when needed.

(j) Activate automated community notification systems, if applicable.

(k) Notify the Virginia Department of Emergency Management Hotline (Va. Code § 44-146.18).

See attachment: 406 USDOT HAZMAT Identification Guidebook.pdf

406.5 REPORTING EXPOSURE

Department members who believe they have been exposed to a hazardous material shall immediately report the exposure to a supervisor. Each exposure shall be documented by the member in an incident report that shall be forwarded via chain of command to the Shift Supervisor as soon as practicable. Should the affected member be unable to document the exposure for any reason, it shall be the responsibility of the notified supervisor to complete the report.

Injury or illness caused or believed to be caused by exposure to hazardous materials shall be reported the same as any other on-duty injury or illness, in addition to a crime report or incident report as applicable.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Hazardous Material Response

406.5.1 SUPERVISOR RESPONSIBILITIES

When a supervisor has been informed that a member has been exposed to a hazardous material, he/she shall ensure that immediate medical treatment is obtained and appropriate action is taken to mitigate the exposure or continued exposure.

To ensure the safety of members, safety equipment is available from supervisors. Safety items not maintained by this department may be available through the appropriate fire department or emergency response team.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Hostage and Barricade Incidents

407.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for situations where deputies have legal cause to contact, detain or arrest a person, and the person refuses to submit to the lawful requests of the deputies by remaining in a structure or vehicle and/or by taking a hostage.

The scope of this policy is not intended to address all variables that deputies encounter during their initial response or when a hostage or barricade situation has developed. This policy does not require or recommend specific strategies or tactics for resolution as each incident is a dynamic and rapidly evolving event.

407.1.1 DEFINITIONS

Definitions related to this policy include:

Barricade situation - An incident where a person maintains a position of cover or concealment and ignores or resists law enforcement personnel, and it is reasonable to believe the subject is armed with a dangerous or deadly weapon.

Hostage situation - An incident where it is reasonable to believe a person is:

- Unlawfully held by a hostage-taker as security so that specified terms or conditions will be met.
- Unlawfully held against his/her will under threat or actual use of force.

Real-time location data - Any data or information concerning the current location of an electronic device (Va. Code § 19.2-70.3).

407.2 POLICY

It is the policy of the Madison County Sheriff's Office to address hostage and barricade situations with due regard for the preservation of life and balancing the risk of injury, while obtaining the safe release of hostages, apprehending offenders and securing available evidence.

407.3 COMMUNICATION

When circumstances permit, initial responding deputies should try to establish and maintain lines of communication with a barricaded person or hostage-taker. Deputies should attempt to identify any additional subjects, inquire about victims and injuries, seek the release of hostages, gather intelligence information, identify time-sensitive demands or conditions and obtain the suspect’s surrender.

When available, department-authorized negotiators should respond to the scene as soon as practicable and assume communication responsibilities. Negotiators are permitted to exercise flexibility in each situation based upon their training, the circumstances presented, suspect actions or demands, and the available resources.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

407.3.1 EMERGENCY COMMUNICATIONS

Deputies who are supervising a hostage or barricade situation may order a telephone company to interrupt, reroute, divert or control any telephone communications service as is reasonably necessary (Va. Code § 18.2-50.2).

During an emergency situation, a deputy may request to track a cell phone or other wireless device without a warrant when (Va. Code § 19.2-70.3(E)):

(a) The deputy reasonably believes that the data is needed to prevent immediate danger to a person and there is not sufficient time to obtain a warrant.

(b) Consent has been given by the owner or user of the phone or next of kin of the owner or user, as applicable.

(c) A call for emergency services has been made from the phone.

Within three days after any such tracking, the deputy should submit a report to the appropriate court detailing the underlying facts that led to the tracking (Va. Code § 19.2-70.3(E)).

407.4 FIRST RESPONDER CONSIDERATIONS

First responding deputies should promptly and carefully evaluate all available information to determine whether an incident involves, or may later develop into, a hostage or barricade situation.

The first responding deputy should immediately request a Shift Supervisor's response as soon as it is determined that a hostage or barricade situation exists. The first responding deputy shall assume the duties of the supervisor until relieved by a supervisor or a more qualified responder. The deputy shall continually evaluate the situation, including the level of risk to deputies, to the persons involved and to bystanders, and the resources currently available.

The handling deputy should brief the arriving supervisor of the incident, including information about suspects and victims, the extent of any injuries, additional resources or equipment that may be needed, and current perimeters and evacuation areas.

407.4.1 BARRICADE SITUATION

Unless circumstances require otherwise, deputies handling a barricade situation should attempt to avoid a forceful confrontation in favor of stabilizing the incident by establishing and maintaining lines of communication while awaiting the arrival of specialized personnel and trained negotiators. In the interim, the following options, while not all-inclusive or in any particular order, should be considered:

(a) Ensure injured persons are evacuated from the immediate threat area if it is reasonably safe to do so. Request medical assistance.

(b) Assign personnel to a contact team to control the subject should he/she attempt to exit the building, structure or vehicle, and attack, use deadly force, attempt to escape or surrender prior to additional resources arriving.

(c) Request additional personnel, resources and equipment as needed (e.g., canine team, air support).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Provide responding emergency personnel with a safe arrival route to the location.

(e) Evacuate uninjured persons in the immediate threat area if it is reasonably safe to do so.

(f) Attempt to obtain a line of communication and gather as much information on the subject as possible, including weapons, other involved parties, additional hazards or injuries.

(g) Establish an inner and outer perimeter as circumstances require and resources permit to prevent unauthorized access.

(h) Evacuate bystanders, residents and businesses within the inner and then outer perimeter as appropriate. Check for injuries, the presence of other involved subjects, witnesses, evidence or additional information.

(i) Determine the need for and notify the appropriate persons within and outside the Department, such as command officers and the Public Information Officer (PIO).

(j) If necessary and available, establish a tactical or exclusive radio frequency for the incident.

(k) Establish a command post.

407.4.2 HOSTAGE SITUATION

Deputies presented with a hostage situation should attempt to avoid a forceful confrontation in favor of controlling the incident in anticipation of the arrival of specialized personnel and trained hostage negotiators. However, it is understood that hostage situations are dynamic and can require that deputies react quickly to developing or changing threats. The following options, while not all-inclusive or in any particular order, should be considered:

(a) Ensure injured persons are evacuated from the immediate threat area if it is reasonably safe to do so. Request medical assistance.

(b) Assign personnel to a contact team to control the subject should he/she attempt to exit the building, structure or vehicle, and attack, use deadly force, attempt to escape or surrender prior to additional resources arriving.

(c) Establish a rapid response team in the event it becomes necessary to rapidly enter a building, structure or vehicle, such as when the suspect is using deadly force against any hostages (see the Rapid Response and Deployment Policy).

(d) Assist hostages or potential hostages to escape if it is reasonably safe to do so. Hostages should be kept separated, if practicable, pending further interview.

(e) Request additional personnel, resources and equipment as needed (e.g., canine team, air support).

(f) Provide responding emergency personnel with a safe arrival route to the location.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(g) Evacuate uninjured persons in the immediate threat area if it is reasonably safe to do so.

(h) Coordinate pursuit or surveillance vehicles and control of travel routes.

(i) Attempt to obtain a line of communication and gather as much information about the suspect as possible, including any weapons, victims and their injuries, additional hazards, other involved parties and any other relevant intelligence information.

(j) Establish an inner and outer perimeter as resources and circumstances permit to prevent unauthorized access.

(k) Evacuate bystanders, residents and businesses within the inner and then outer perimeter as appropriate. Check for injuries, the presence of other involved subjects, witnesses, evidence or additional information.

(l) Determine the need for and notify the appropriate persons within and outside the Department, such as command officers and the PIO.

(m) If necessary and available, establish a tactical or exclusive radio frequency for the incident.

407.5 SUPERVISOR RESPONSIBILITIES

Upon being notified that a hostage or barricade situation exists, the Shift Supervisor should immediately respond to the scene, assess the risk level of the situation, establish a proper chain of command and assume the role of Incident Commander until properly relieved. This includes requesting Crisis Response Unit (CRU) response if appropriate and apprising the CRU Commander of the circumstances. In addition, the following options, listed here in no particular order, should be considered:

(a) Ensure injured persons are evacuated and treated by medical personnel.

(b) Ensure the completion of necessary first responder responsibilities or assignments.

(c) Request crisis negotiators, specialized assignment members, additional department members, resources, or equipment as appropriate.

(d) Establish a command post location as resources and circumstances permit.

(e) Designate assistants who can help with intelligence information and documentation of the incident.

(f) If it is practicable to do so, arrange for video documentation of the operation.

(g) Consider contacting utility and communication providers when restricting such services (e.g., electric power, gas, telephone service).

(h) Ensure adequate law enforcement coverage for the remainder of the County during the incident. The Shift Supervisor should direct nonessential personnel away from the scene unless they have been summoned by the supervisor or the Dispatch Center.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(i) Identify a media staging area outside the outer perimeter and have the department PIO or a designated temporary media representative provide media access in accordance with the Media Relations Policy.

(j) Identify the need for mutual aid and the transition or relief of personnel for incidents of extended duration.

(k) Debrief personnel and review documentation as appropriate.

407.6 CRU RESPONSIBILITIES

It will be the CRU Commander's decision, with input from the Incident Commander, whether to deploy the CRU during a hostage or barricade situation. Once the CRU Commander authorizes deployment, the CRU Commander or the authorized designee will be responsible for the tactical response and negotiations. The Incident Commander shall continue to supervise the command post operation, outer perimeter security, evacuation and media access, and will support the CRU. The Incident Commander and the CRU Commander or the authorized designees shall maintain direct communications at all times.

407.7 REPORTING

Unless otherwise relieved by a Shift Supervisor or Incident Commander, the handling deputy at the scene is responsible for completion and/or coordination of incident reports.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Response to Bomb Calls

408.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines to assist members of the Madison County Sheriff's Office in their initial response to incidents involving explosives or explosive devices, explosion/bombing incidents or threats of such incidents. Under no circumstances should these guidelines be interpreted as compromising the safety of first responders or the public. When confronted with an incident involving explosives, safety should always be the primary consideration.

408.2 POLICY

It is the policy of the Madison County Sheriff's Office to place a higher priority on the safety of persons and the public over damage or destruction to public or private property.

408.3 RECEIPT OF BOMB THREAT

Department members receiving a bomb threat should obtain as much information from the individual as reasonably possible, including the type, placement, and alleged detonation time of the device.

If the bomb threat is received on a recorded line, reasonable steps should be taken to ensure that the recording is preserved in accordance with established department evidence procedures.

The member receiving the bomb threat should ensure that the Shift Supervisor is immediately advised and informed of the details. This will enable the Shift Supervisor to ensure that the appropriate personnel are dispatched, and, as appropriate, the threatened location is given an advance warning.

See attachment: 408 Bomb Threat Procedures and Checklist.pdf

408.4 GOVERNMENT FACILITY OR PROPERTY

A bomb threat targeting a government facility may require a different response based on the government agency.

408.4.1 MADISON COUNTY SHERIFF'S OFFICE FACILITY

If the bomb threat is against the Madison County Sheriff's Office facility, the Shift Supervisor will direct and assign deputies as required for coordinating a general building search or evacuation of the sheriff's department, as he/she deems appropriate.

408.4.2 OTHER COUNTY OR MUNICIPAL FACILITY OR PROPERTY

If the bomb threat is against a county or municipal facility within the jurisdiction of the Madison County Sheriff's Office that is not the property of this department, the appropriate agency will be promptly informed of the threat. Assistance to the other entity may be provided as the Shift Supervisor deems appropriate.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

408.4.3 FEDERAL BUILDING OR PROPERTY

If the bomb threat is against a federal building or property, the Federal Protective Service should be immediately notified. The Federal Protective Service provides a uniformed law enforcement response for most facilities, which may include use of its Explosive Detector Dog teams.

If the bomb threat is against a federal government property where the Federal Protective Service is unable to provide a timely response, the appropriate facility's security or command staff should be notified.

Bomb threats against a military installation should be reported to the military police or other military security responsible for the installation.

408.5 PRIVATE FACILITY OR PROPERTY

When a member of this department receives notification of a bomb threat at a location in the County of Madison County, Virginia, the member receiving the notification should obtain as much information as reasonably possible from the notifying individual, including:

(a) The location of the facility.

(b) The nature of the threat.

(c) Whether the type and detonation time of the device is known.

(d) Whether the facility is occupied and, if so, the number of occupants currently on-scene.

(e) Whether the individual is requesting sheriff's assistance at the facility.

Whether there are any internal facility procedures regarding bomb threats in place, such as:

(a) No evacuation of personnel and no search for a device.

(b) Search for a device without evacuation of personnel.

(c) Evacuation of personnel without a search for a device.

(d) Evacuation of personnel and a search for a device.

The member receiving the bomb threat information should ensure that the Shift Supervisor is immediately notified so that he/she can communicate with the person in charge of the threatened facility.

408.5.1 ASSISTANCE

The Shift Supervisor should be notified when sheriff's assistance is requested. The Shift Supervisor will make the decision whether the Department will render assistance and at what level. Information and circumstances that indicate a reasonably apparent, imminent threat to the safety of either the facility or the public may require a more active approach, including sheriff's control over the facility.

Should the Shift Supervisor determine that the Department will assist or control such an incident, they will determine:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) The appropriate level of assistance.

(b) The plan for assistance.

(c) Whether to evacuate and/or search the facility.

(d) Whether to involve facility staff in the search or evacuation of the building.

1. The person in charge of the facility should be made aware of the possibility of damage to the facility as a result of a search.
2. The safety of all participants is the paramount concern.

(e) The need for additional resources, including:

1. Notification and response, or standby notice, for fire and emergency medical services.

Even though a facility does not request sheriff's assistance to clear the interior of a building, based upon the circumstances and known threat, deputies may be sent to the scene to evacuate other areas that could be affected by the type of threat, or for traffic and pedestrian control.

408.6 FOUND DEVICE

When handling an incident involving a suspected explosive device, the following guidelines, while not all inclusive, should be followed:

(a) No known or suspected explosive item should be considered safe regardless of its size or apparent packaging.

(b) The device should not be touched or moved except by the bomb squad or military explosive ordnance disposal team.

(c) Personnel should not transmit on any equipment that is capable of producing radio frequency energy within the evacuation area around the suspected device. This includes:

1. Two-way radios.
2. Cell phones.
3. Other personal communication devices.

(d) The appropriate bomb squad or military explosive ordnance disposal team should be summoned for assistance.

(e) The largest perimeter reasonably possible should initially be established around the device based upon available personnel and the anticipated danger zone.

(f) A safe access route should be provided for support personnel and equipment.

(g) Search the area for secondary devices as appropriate and based upon available resources.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(h) Consider evacuation of buildings and personnel near the device or inside the danger zone and the safest exit route.

(i) Promptly relay available information to the Shift Supervisor including:

1. The time of discovery.
2. The exact location of the device.
3. A full description of the device (e.g., size, shape, markings, construction).
4. The anticipated danger zone and perimeter.
5. The areas to be evacuated or cleared.

408.7 EXPLOSION/BOMBING INCIDENTS

When an explosion has occurred, there are multitudes of considerations that may confront the responding deputies. As in other catastrophic events, a rapid response may help to minimize injury to victims, contamination of the scene by gathering crowds, or any additional damage from fires or unstable structures.

408.7.1 CONSIDERATIONS

Deputies responding to explosions, whether accidental or a criminal act, should consider the following actions:

(a) Assess the scope of the incident, including the number of victims and extent of injuries.

(b) Request additional personnel and resources, as appropriate.

(c) Assist with first aid.

(d) Identify and take appropriate precautions to mitigate scene hazards, such as collapsed structures, bloodborne pathogens and hazardous materials.

(e) Assist with the safe evacuation of victims, if possible.

(f) Establish an inner perimeter to include entry points and evacuation routes. Search for additional or secondary devices.

(g) Preserve evidence.

(h) Establish an outer perimeter and evacuate if necessary.

(i) Identify witnesses.

408.7.2 NOTIFICATIONS

When an explosion has occurred, the following people should be notified as appropriate:

- Fire department
- The Virginia State Police bomb squad
- Additional department personnel, such as investigators and forensic services

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

- Field supervisor
- Shift Supervisor
- Other law enforcement agencies, including local, state or federal agencies, such as the FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
- Other government agencies, as appropriate

408.8 CROWD CONTROL

Only authorized members with a legitimate need should be permitted access to the scene. Spectators and other unauthorized individuals should be restricted to a safe distance as is reasonably practicable given the available resources and personnel.

408.8.1 PRESERVATION OF EVIDENCE

As in any other crime scene, steps should immediately be taken to preserve the scene. The Shift Supervisor should assign deputies to protect the crime scene area, which could extend over a long distance. Consideration should be given to the fact that evidence may be embedded in nearby structures or hanging in trees and bushes.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Crisis Intervention Incidents

409.1 PURPOSE AND SCOPE

This policy provides guidelines for interacting with those who may be experiencing a mental health crisis pr suffering from mental illness. Interaction with such individuals has the potential for miscommunication and violence. It often requires a deputy to make difficult judgments about a person's mental state and intent in order to effectively and legally interact with the individual.

409.1.1 DEFINITIONS

Definitions related to this policy include:

Co-Responder – A behavioral health specialist who is paired with law enforcement to intervene and respond to behavioral health related calls for service.

Marcus Alert - The Marcus-David Peters Act is a comprehensive approach to ensuring that Virginia provides a therapeutic, health-focused response to behavioral health emergencies. The Act includes coordination between recent investments in the behavioral health crisis continuum, including mobile crisis teams to respond statewide 24/7, protocols that focus on full diversion to the behavioral health system, specific requirements for mobile crisis and law enforcement when law enforcement is called as back-up, protocols to guide any co-response programs or other community care models, and protocols regarding police presentation, training, and behavior such as use of force whenever responding to a behavioral health emergency.

Mental Health Crisis -An event or experience in which an individual's normal coping mechanisms are overwhelmed, causing them to have an extreme emotional, physical, mental, and/or behavioral response. Symptoms may include emotional reactions such as fear, anger, or excessive giddiness; psychological impairments such as inability to focus, confusion, or nightmares, and potentially even psychosis; physical reactions like vomiting/stomach issues, headaches, dizziness, excessive tiredness, or insomnia; and/or behavioral reactions including the trigger of a "freeze, fight, or flight" response. Any individual can experience a crisis reaction regardless of previous history of mental illness.

Mental Illness - An impairment of an individual's normal cognitive, emotional, or behavioral functioning, caused by physiological or psychosocial factors. A person may be affected by mental illness if they display an inability to think rationally (e.g., delusions or hallucinations); exercise adequate control over behavior or impulses (e.g., aggressive, suicidal, homicidal, sexual); and/or take reasonable care of their welfare with regard to basic provisions for clothing, food, shelter, or safety.

Peer Specialist - Certified Peer Recovery Specialists (CPRS) provide non-clinical, person-centered, strengths based, wellness focused, and trauma-informed support while partnering with someone in the development of their wellness-recovery plan.

Person in crisis (PIC) - A person whose level of distress or mental health symptoms have exceeded the person's internal ability to manage his/her behavior or emotions. A crisis can be

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

precipitated by any number of things, including an increase in the symptoms of mental illness despite treatment compliance; noncompliance with treatment, including a failure to take prescribed medications appropriately; or any other circumstance or event that causes the person to engage in erratic, disruptive or dangerous behavior that may be accompanied by impaired judgment.

409.2 POLICY

The Madison County Sheriff's Office is committed to providing a consistently high level of service to all members of the community and recognizes that persons in crisis may benefit from intervention. The Department will collaborate, where feasible, with mental health professionals to develop an overall intervention strategy to guide its members' interactions with those experiencing a mental health crisis. This is to ensure equitable and safe treatment of all involved.

It is the policy of the Madison County Sheriff's Office that appropriate referrals for treatment of mental illness or crisis intervention should be sought when no serious crime has been committed and no danger is presented to the public. When public safety demands otherwise, it may be necessary to resort to involuntary detentions and or arrest. Nothing in this directive shall prohibit sworn personnel from initiating criminal arrest procedures whenever appropriate.

409.3 SIGNS

Officers are not expected to diagnose mental or emotional conditions, but rather to recognize behaviors that are potentially indicative of a PIC, with special emphasis on those that suggest potential violence and/or danger. The following are generalized signs and symptoms of behavior that may suggest an individual is experiencing a mental health crisis, but each should be evaluated within the context of the entire situation:

(a) A known history of mental illness

(b) Threats of or attempted suicide

(c) Loss of memory

(d) Incoherence, disorientation or slow response

(e) Delusions, hallucinations, perceptions unrelated to reality or grandiose ideas

(f) Depression, pronounced feelings of hopelessness or uselessness, extreme sadness or guilt

(g) Social withdrawal

(h) Manic or impulsive behavior, extreme agitation or lack of control

(i) Lack of fear

(j) Anxiety, aggression, rigidity, inflexibility or paranoia

(k) Nonsensical speech patterns

(l) Dramatic changes in eating or sleeping habits

(m) Increasing inability to cope with daily problems

(n) Denial of obvious problems

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(o) Many unexplained physical problems

(p) Abuse of alcohol or drugs

Members should be aware that this list is not exhaustive. The above signs may display themselves in verbal, environmental and behavioral indicators exhibited by a person suffering from a mental illness. Deputies should evaluate these indicators in the totality of the context in which they occur in order to assess an individual's mental state and the need for law enforcement intervention absent the commission of a crime. The presence or absence of any of these signs should not be treated as proof of the presence or absence of a mental health issue or crisis.

Madison County Sheriff's Office Law Enforcement Procedures Manual: 406.1 Indicators of Mental Illness

409.4 ASSESSING RISK

Most PICs are not violent and some may present dangerous behavior only under certain circumstances or conditions. Officers may use several indicators to assess whether a PIC represents potential danger to themselves, the police, or others. These include the following:

(a) The availability of any weapons.

(b) Threats of harm to self or others or statements by the person that suggest that they are prepared to commit a violent or dangerous act. Such comments may range from subtle innuendo to direct threats that, when taken in conjunction with other information, paint a more complete picture of the potential for violence.

(c) A personal history that reflects prior violence under similar or related circumstances. The person's history may already be known to the officer, or family, friends, or neighbors might provide such information.

(d) The amount of self-control that the person exhibits, particularly the amount of physical control, over emotions such as rage, anger, fright, or agitation. Signs of a lack of self-control include extreme agitation, inability to sit still or communicate effectively, wide eyes, and rambling thoughts and speech. Clutching oneself or other objects to maintain control, begging to be left alone, or offering frantic assurances that one is all right may also suggest that the individual is close to losing control.

(e) Indications of substance use, as these may alter the individual's self-control and negatively influence an officer's capacity to effectively use de-escalation strategies.

(f) The volatility of the environment. Agitators that may affect the person or create a particularly combustible environment or incite violence should be taken into account and mitigated. For example, the mere presence of a law enforcement vehicle, an officer in uniform, and/or a weapon may be seen as a threat to a PIC and has the potential to escalate a situation. Standard law enforcement tactics may need to be modified to accommodate the situation when responding to a PIC.

(g) Aggressive behaviors such as advancing on or toward an officer, refusal to follow directions or commands combined with physical posturing, and verbal or nonverbal threats.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Failure to exhibit violent or dangerous behavior prior to the arrival of the officer does not guarantee that there is no danger. Context is crucial in the accurate assessment of behavior. Officers should take into account the totality of circumstances requiring their presence and overall need for intervention.

409.5 COORDINATION WITH MENTAL HEALTH PROFESSIONALS

The Sheriff should collaborate with mental health professionals to develop an education and response protocol. It should include a list of community resources to guide department interaction with those who may be suffering from mental illness or who appear to be in a mental health crisis (Va. Code § 9.1-187).

Madison County Sheriff's Office Law Enforcement Procedures Manual: 407.1 Mental Health/ Substance Abuse Resources

409.6 FIRST RESPONDERS

Safety is a priority for first responders. It is important to recognize that individuals under the influence of alcohol, drugs or both may exhibit symptoms that are similar to those of a person in a mental health crisis. These individuals may still present a serious threat to deputies; such a threat should be addressed with reasonable tactics. Nothing in this policy shall be construed to limit a deputy's authority to use reasonable force when interacting with a person in crisis.

Deputies are reminded that mental health issues, mental health crises and unusual behavior are not criminal offenses. Individuals may benefit from treatment as opposed to incarceration.

Upon receipt of a call for service involving an apparent mental health or emotional crisis, the on-duty Rappahannock Rapidan Community Services Board (CSB)co-responder shall be notified. A Crisis Intervention Trained (CIT) trained law enforcement deputy shall be dispatched to the scene, if available. Additional law enforcement resources should also be dispatched to the scene as required.

The CIT trained deputy or other law enforcement personnel responding to a call involving a person in crisis should:

(a) Promptly assess the situation independent of reported information and make a preliminary determination regarding whether a mental health crisis may be a factor.

(b) Request available backup deputies and specialized resources as deemed necessary and, if it is reasonably believed that the person is in a crisis situation, use conflict resolution and de-escalation techniques to stabilize the incident as appropriate.

(c) If feasible, and without compromising safety, turn off flashing lights, bright lights or sirens.

(d) Attempt to determine if weapons are present or available.

(e) Take into account the person's mental and emotional state and potential inability to understand commands or to appreciate the consequences of his/her action or inaction, as perceived by the deputy.

(f) Secure the scene and clear the immediate area as necessary.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(g) Employ tactics to preserve the safety of all participants.

(h) Determine the nature of any crime.

(i) Request a supervisor, as warranted.

(j) Evaluate any available information that might assist in determining cause or motivation for the person's actions or stated intentions.

(k) If circumstances reasonably permit, consider and employ alternatives to force.

The CSB co-responder shall not enter the premises unless the assigned deputy indicates that it is safe to do so. Once it is safe to do so, the CSB co-responder will interact with the individual and then discuss the best course of action with the deputy. Deputies will permit the CSB to assume primary contact with the subject.Deputies will remain on the scene to maintain order as necessary, and will assist in supporting the CSB by providing transportation or other resources as may be required. The CSB shall disclose to law enforcement personnel all health information necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public (45 CFR 164.512(j)(1)(i)(A)). Once the CSB Representative is no longer needed then they may clear the scene.

In the event that the prevailing issue is medical treatment, as in the cases of overdose and self-inflicted injuries, etc. EMS/Rescue medical personnel shall be requested via the Communication Center immediately.

409.6.1 VOLUNTARY ADMISSION/REFERRAL TO MENTAL HEALTH PRACTITIONERS

(a) Persons who appear to be in need of mental health treatment, but who have not committed a crime, and do not pose an imminent danger to themselves or others, should be referred to a medical or mental health facility, evaluator or practitioner.

(b) Whenever possible, a family member or other responsible person, who agrees to assist the disturbed person in seeking such treatment, should be located. Often these persons help distinguish between those disturbed persons who already have a physician to follow-up, and those requiring immediate care and intervention

(c) Persons that have been or are presently under the care of a private physician should be referred to that physician, if possible

(d) A voluntary admission for treatment is preferable to an involuntary admission in most cases

(e) In the event that the person initially seeking voluntary admission to a mental health facility decided against this course of action, the procedure for an involuntary admission procedure shall be followed

(f) Once proper referral information is provided to the individual and/or their family, and the individual does not pose an imminent danger to themselves or others, the deputy shall clear from the scene

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Juveniles should be handled in the same manner as adults for purposes of identifying the need for referral to a medical or mental health facility, evaluator or practitioner for mental health treatment or crisis intervention.

409.6.2 INVOLUNTARY ADMISSION PROCEDURES
Refer to Civil Commitments policy.

409.7 DE-ESCALATION

Deputies should consider that taking no action or passively monitoring the situation may be the most reasonable response to a mental health crisis.

Once it is determined that a situation is a mental health crisis and immediate safety concerns have been addressed, responding members should be aware of the following considerations and should generally:

- Evaluate safety conditions.
- Introduce themselves and attempt to obtain the person’s name.
- Be patient, polite, calm and courteous and avoid overreacting.
- Speak and move slowly and in a non-threatening manner.
- Moderate the level of direct eye contact.
- Remove distractions or disruptive people from the area.
- Demonstrate active listening skills (i.e., summarize the person’s verbal communication).
- Provide for sufficient avenues of retreat or escape should the situation become volatile.

Responding deputies generally should not:

- Use stances or tactics that can be interpreted as aggressive.
- Allow others to interrupt or engage the person.
- Corner a person who is not believed to be armed, violent or suicidal.
- Argue, speak with a raised voice or use threats to obtain compliance.

409.8 INCIDENT ORIENTATION

When responding to an incident that may involve mental illness or a mental health crisis, the deputy should request that the dispatcher provide critical information as it becomes available. This includes:

(a) Whether the person relies on drugs or medication, or may have failed to take his/her medication.

(b) Whether there have been prior incidents or suicide threats/attempts, and whether there has been previous sheriff's response.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) Contact information for a treating physician or mental health professional.

Additional resources and a supervisor should be requested as warranted.

409.9 SUPERVISOR RESPONSIBILITIES

A supervisor should respond to the scene of any interaction with a person in crisis. Responding supervisors should:

(a) Attempt to secure appropriate and sufficient resources.

(b) Closely monitor any use of force, including the use of restraints, and ensure that those subjected to the use of force are provided with timely access to medical care (see the Handcuffing and Restraints Policy).

(c) Absent an imminent threat to the public, consider strategic disengagement. This may include removing or reducing law enforcement resources or engaging in passive monitoring.

(d) Ensure that all reports are completed and that incident documentation uses appropriate terminology and language.

(e) Conduct an after-action tactical and operational debriefing, and prepare an after-action evaluation of the incident to be forwarded to the Division Supervisor.

(f) Evaluate whether a critical incident stress management debriefing for involved members is warranted.

409.10 INCIDENT REPORTING

Members engaging in any oral or written communication associated with a mental health crisis should be mindful of the sensitive nature of such communications and should exercise appropriate discretion when referring to or describing persons and circumstances.

Members having contact with a person in crisis should keep related information confidential, except to the extent that revealing information is necessary to conform to department reporting procedures or other official mental health or medical proceedings.

409.10.1 DIVERSION

Individuals who are not being arrested should be processed in accordance with the Civil Commitments Policy.

Members encountering a person who is sufficiently stable, and who is not arrested or committed, should provide information and direction for appropriate emergency self-help treatment services (Va. Code § 9.1-189).

409.11 NON-SWORN INTERACTION WITH PEOPLE IN CRISIS

Non-sworn or clerical members may be required to interact with persons in crisis in an administrative capacity, such as dispatching, records request and animal control issues.

(a) Members should treat all individuals equally and with dignity and respect.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) If a member believes that he/she is interacting with a person in crisis, he/she should proceed patiently and in a calm manner.

(c) Members should be aware and understand that the person may make unusual or bizarre claims or requests.

If a person's behavior makes the member feel unsafe, if the person is or becomes disruptive or violent, or if the person acts in such a manner as to cause the member to believe that the person may be harmful to him/herself or others, a deputy should be promptly summoned to provide assistance.

409.12 EVALUATION

The Division Supervisor designated to coordinate the crisis intervention strategy for this department should ensure that a thorough review and analysis of the department response to these incidents is conducted annually. The report will not include identifying information pertaining to any involved individuals, deputies or incidents and will be submitted to the Sheriff through the chain of command.

409.13 TRAINING

In coordination with the mental health community and appropriate stakeholders, the Department will develop and provide comprehensive education and training to all department members to enable them to effectively interact with persons in crisis.

Deputies specifically assigned to a crisis intervention team shall successfully complete training as required by the Department of Criminal Justice Services (DCJS) (Va. Code § 9.1-188).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Civil Commitments

410.1 PURPOSE AND SCOPE

This policy provides guidelines for when deputies may place a person under an emergency custody civil commitment.

410.2 POLICY

It is the policy of the Madison County Sheriff's Office to protect the public and individuals through legal and appropriate use of the civil commitment process.

410.3 AUTHORITY

A deputy, based upon his/her observations or the reliable report of others, may take a person into emergency custody for a civil commitment when there is probable cause to believe a person meets the criteria established by state law, which include (Va. Code § 16.1-340(G); Va. Code § 37.2-808(G)):

(a) The person has a mental illness and because of that mental illness, either:

1. Is a danger to him/herself or others, as evidenced by recent conduct.
2. Is unable to care for him/herself or to protect him/herself from harm.

(b) The person is in need of treatment.

(c) The person is unwilling to volunteer or incapable of volunteering for treatment.

If a deputy takes a person into emergency custody for a civil commitment, the deputy shall transport the person to an appropriate designated location to assess the need for hospitalization or treatment. The deputy shall ensure that the Community Services Board (CSB) responsible for conducting the evaluation is notified as soon as practicable once the person is taken into custody (Va. Code § 16.1-340(I); Va. Code § 37.2-808(J)).

The period of custody shall not exceed eight hours from the time the law-enforcement officer takes the person into custody (Va. Code §37.2-808(H)).

An adult taken into emergency custody for a civil commitment shall be provided with a written summary of the emergency custody procedures and the statutory protections associated with those procedures (Va. Code § 37.2-808(M)).

A deputy shall also take a person into custody when a court order is issued by any magistrate authorizing emergency custody or temporary detention for a civil commitment. The deputy shall then transport the person to the designated medical facility or transfer custody of the person to the alternative transportation provider identified in the order (Va. Code § 16.1-340; Va. Code § 16.1-340.1; Va. Code § 16.1-340.2; Va. Code § 37.2-808; Va. Code § 37.2-809; Va. Code § 37.2-810).

Madison County Sheriff's Office Law Enforcement Procedures Manual: 408.1 Procedures for Emergency and Temporary Custody Orders

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

See attachment: CITAC Business Hours.pdf

See attachment: Rappahannock Rapidan MOU re Transfer of Custody.pdf

See attachment: Rappahannock Rapidan Transfer of Custody Form.pdf

See attachment: Rappahannock Rapidan Community Services MOU.pdf

410.3.1 VOLUNTARY EVALUATION

If a deputy encounters an individual who may qualify for a civil commitment, he/she may inquire as to whether the person desires to be voluntarily evaluated at an appropriate facility. If the person so desires, the deputy should:

(a) Transport the person to an appropriate facility that is able to conduct the evaluation and admit the person.

(b) Document the circumstances surrounding the individual's desire to pursue voluntary evaluation and/or admission.

(c) Make arrangements for the person to transported by EMS to an appropriate facility.

If at any point the person changes his/her mind regarding voluntary evaluation, the deputies should proceed with an emergency custody for civil commitment evaluation, if appropriate (Va. Code § 16.1-340; Va. Code § 37.2-808).

The deputy shall ensure that the CSB responsible for conducting the voluntary evaluation is notified as soon as practicable once the person is taken into custody (Va. Code § 16.1-340(I); Va. Code § 37.2-808(J)).

410.4 CONSIDERATIONS AND RESPONSIBILITIES

Any deputy handling a call involving a person who may qualify for detention for the purpose of civil commitment should consider, as time and circumstances reasonably permit:

(a) Available information that might assist in determining the possible cause and nature of the person’s action or stated intentions.

(b) Community or neighborhood mediation services.

(c) Conflict resolution and de-escalation techniques.

(d) Community or other resources that may be readily available to assist with mental health issues.

(e) Crisis intervention team programs (Va. Code § 9.1-187).

While these steps are encouraged, nothing in this section is intended to dissuade deputies from taking reasonable action to ensure the safety of the deputies and others.

Civil commitments should be preferred over arrest for people who have mental health issues and are suspected of committing minor crimes or creating other public safety issues.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

410.5 TRANSPORTATION

When transporting any individual for a civil commitment, the transporting deputy should have the Dispatch Center notify the receiving facility of the estimated time of arrival, the level of cooperation of the individual and whether any special medical care is needed.

Deputies may transport individuals in the patrol unit and shall secure them in accordance with the Handcuffing and Restraints Policy. Should the detainee require transport in a medical transport vehicle and the safety of any person, including the detainee, requires the presence of a deputy during the transport, Shift Supervisor approval is required before transport commences.

410.6 TRANSFER TO APPROPRIATE FACILITY

Upon arrival at the facility, the deputy will escort the individual into a treatment area designated by a facility staff member. If the individual is not seeking treatment voluntarily, the deputy should provide the staff member with the written application for a civil commitment and remain present to provide clarification of the grounds for detention, upon request.

Absent exigent circumstances, the transporting deputy should not assist facility staff with the admission process, including restraint of the individual. However, if the individual is transported and delivered while restrained, the deputy may assist with transferring the individual to facility restraints and will be available to assist during the admission process, if requested. Under normal circumstances, deputies will not apply facility-ordered restraints.

410.7 DOCUMENTATION

The deputy should complete all applicable forms for the emergency custody for civil commitment, provide it to the facility staff member assigned to the individual and retain a copy for inclusion in the case report.

The deputy should also provide a verbal summary to any evaluating staff member regarding the circumstances leading to the involuntary detention.

The deputy should notify a supervisor regarding the circumstances of the incident and the action taken during the investigation.

410.8 CRIMINAL OFFENSES

Deputies investigating an individual who is suspected of committing a minor criminal offense and who is being taken into custody for a civil commitment should resolve the criminal matter by issuing a warning or a citation, as appropriate.

When an individual who may qualify for a civil commitment has committed a serious criminal offense that would normally result in an arrest and transfer to a jail facility, the deputy should:

(a) Arrest the individual when there is probable cause to do so.

(b) Notify the appropriate supervisor of the facts supporting the arrest and the facts that would support the detention.

(c) Facilitate the individual’s transfer to jail.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Thoroughly document in the related reports the circumstances that indicate the individual may qualify for a civil commitment.

In the supervisor's judgment, the individual may instead be transported to the appropriate mental health facility. The supervisor should consider the seriousness of the offense, the treatment options available, the ability of this department to regain custody of the individual, department resources (e.g., posting a guard), and other relevant factors in making this decision.

410.9 FIREARMS AND OTHER WEAPONS

Whenever a person is taken into custody for a civil commitment, the handling deputies should seek to determine if the person owns or has access to any firearm or other deadly weapon. Deputies should consider whether it is appropriate and consistent with current search and seizure law under the circumstances to seize any such firearms or other dangerous weapons (e.g., safekeeping, evidence, consent).

Deputies are cautioned that a search warrant may be needed before entering a residence or other place to search, unless lawful warrantless entry has already been made (e.g., exigent circumstances, consent). A warrant may also be needed before searching for or seizing weapons.

The handling deputy should further advise the person of the procedure for the return of any firearm or other weapon that has been taken into custody.

410.10 TRAINING

This department will endeavor to provide department-approved training on interaction with mentally disabled persons, civil commitments and crisis intervention.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Citation Releases

411.1 PURPOSE AND SCOPE

The purpose of this policy is to provide members of the Madison County Sheriff's Office with guidance on when to release adults who are suspected offenders on a summons for a criminal offense, rather than having the person held in custody for a court appearance or released on bail.

Additional release restrictions may apply to those detained for domestic violence, as outlined in the Domestic or Family Violence Policy.

411.2 POLICY

The Madison County Sheriff's Office will consider its resources and its mission of protecting the community when exercising any discretion to release suspected offenders on a summons, when authorized to do so.

411.3 RELEASE

A suspected offender shall be released in the field on a summons for any misdemeanor violation of the Code of Virginia or local ordinance unless there is a statutory exception allowing a full custodial arrest. These exceptions include driving a vehicle while intoxicated, public drunkenness, a warrant authorizing custody, or circumstances where a deputy can articulate a reasonable belief that the person arrested will continue to commit the unlawful act (Va. Code § 19.2-74).

Full custodial arrests for misdemeanors punishable by jail may be made if the deputy can articulate a reasonable belief that the person will fail to appear in court on the person's promise to appear in court. This may include those instances where a person is attempting to hide the person's identity. Full custodial arrests may also be made if the deputy can articulate a reasonable belief that the person is likely to cause harm to the person or to any other person.

Full custodial arrest shall be made if the person refuses to give a written promise to appear (Va. Code § 19.2-74).

411.4 CONSIDERATIONS

In determining whether to release a person on a promise to appear in court and when discretion is permitted, deputies should consider:

(a) The type of offense committed.

(b) The known criminal history of the suspected offender.

(c) The ability to identify the suspected offender with reasonable certainty.

(d) Whether there is any record of the individual failing to appear in previous cases or other articulable indications that the individual may not appear in court for this offense.

(e) The individual’s ties to the area, such as residence, employment or family.

(f) Whether there is reasonable likelihood that criminal conduct by the individual will continue.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Foreign Diplomatic and Consular Representatives

412.1 PURPOSE AND SCOPE

This policy provides guidelines to ensure that members of the Madison County Sheriff's Office extend appropriate privileges and immunities to foreign diplomatic and consular representatives in accordance with international law.

412.2 POLICY

The Madison County Sheriff's Office respects international laws related to the special privileges and immunities afforded foreign diplomatic and consular representatives assigned to the United States.

All foreign diplomatic and consular representatives shall be treated with respect and courtesy, regardless of any privileges or immunities afforded them.

412.3 CLAIMS OF IMMUNITY

If a member comes into contact with a person where law enforcement action may be warranted and the person claims diplomatic or consular privileges and immunities, the member should, without delay:

(a) Notify a supervisor.

(b) Advise the person that his/her claim will be investigated and he/she may be released in accordance with the law upon confirmation of the person’s status.

(c) Request the person’s identification card, either issued by the U.S. Department of State (DOS), Office of the Chief of Protocol or, in the case of persons accredited to the United Nations, by the U.S. Mission to the United Nations. These are the only reliable documents for purposes of determining privileges and immunities.

(d) Contact the DOS Diplomatic Security Command Center at 571–345–3146 or toll-free at 866–217–2089, or at another current telephone number, and inform the center of the circumstances.

(e) Verify the immunity status with DOS and follow any instructions regarding further detention, arrest, prosecution and/or release, as indicated by the DOS representative. This may require immediate release, even if a crime has been committed.

Identity or immunity status should not be presumed from the type of license plates displayed on a vehicle. If there is a question as to the status or the legitimate possession of a Diplomat or Consul license plate, a query should be run via the National Law Enforcement Telecommunications System (NLETS), designating "US" as the state.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

412.4 ENFORCEMENT ACTION

If the DOS is not immediately available for consultation regarding law enforcement action, members shall be aware of the following:

(a) Generally, all persons with diplomatic and consular privileges and immunities may be issued a citation or notice to appear. However, the person may not be compelled to sign the citation.

(b) All persons, even those with a valid privilege or immunity, may be reasonably restrained in exigent circumstances for purposes of self-defense, public safety or the prevention of serious criminal acts.

(c) An impaired foreign diplomatic or consular representative may be prevented from driving a vehicle, even if the person may not be arrested due to privileges and immunities.

1. Investigations, including the request for field sobriety tests, chemical tests and any other tests regarding impaired driving may proceed but they shall not be compelled.

(d) The following persons may not be detained or arrested, and any property or vehicle owned by these persons may not be searched or seized:

1. Diplomatic-level staff of missions to international organizations and recognized family members
2. Diplomatic agents and recognized family members
3. Members of administrative and technical staff of a diplomatic mission and recognized family members
4. Career consular officers, unless the person is the subject of a felony warrant

(e) The following persons may generally be detained and arrested:

1. International organization staff; however, some senior officers are entitled to the same treatment as diplomatic agents
2. Support staff of missions to international organizations
3. Diplomatic service staff and consular employees; however, special bilateral agreements may exclude employees of certain foreign countries
4. Honorary consular officers

412.5 DOCUMENTATION

All contacts with persons who have claimed privileges and immunities afforded foreign diplomatic and consular representatives should be thoroughly documented and the related reports forwarded to DOS.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

412.6 DIPLOMATIC IMMUNITY

Reference table on diplomatic immunity:

Category	Arrested or Detained	Enter Residence Subject to Ordinary Procedures	Issued Traffic Citation	Subpoenaed as Witness	Prosecuted	Recognized Family Members
Diplomatic Agent	No (note (b))	No	Yes	No	No	Same as sponsor (full immunity & inviolability)
Member of Admin and Tech Staff	No (note (b))	No	Yes	No	No	Same as sponsor (full immunity & inviolability)
Service Staff	Yes (note (a))	Yes	Yes	Yes	No for official acts Yes otherwise (note (a))	No immunity or inviolability (note (a))
Career Consul Officer	Yes if for a felony and pursuant to a warrant (note (a))	Yes (note (d))	Yes	No for official acts Testimony may not be compelled in any case	No for official acts Yes otherwise (note (a))	No immunity or inviolability
Honorable Consul Officer	Yes	Yes	Yes	No for official acts Yes otherwise	No for official acts Yes otherwise	No immunity or inviolability
Consulate Employees	Yes (note (a))	Yes	Yes	No for official acts Yes otherwise	No for official acts Yes otherwise (note (a))	No immunity or inviolability (note (a))
Int'l Org Staff (note (b))	Yes (note (c))	Yes (note (c))	Yes	Yes (note (c))	No for official acts Yes otherwise (note (c))	No immunity or inviolability

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Foreign Diplomatic and Consular Representatives

Diplomatic-Level Staff of Missions to Int'l Org	No (note (b))	No	Yes	No	No	Same as sponsor (full immunity and inviolability)
Support Staff of Missions to Int'l Orgs	Yes	Yes	Yes	Yes	No for official acts Yes otherwise	No immunity or inviolability

Notes for diplomatic immunity table:

(a) This table represents general rules. The employees of certain foreign countries may enjoy higher levels of privileges and immunities on the basis of special bilateral agreements.

(b) Reasonable constraints, however, may be applied in emergency circumstances involving self-defense, public safety or the prevention of serious criminal acts.

(c) A small number of senior officers are entitled to be treated identically to diplomatic agents.

(d) Note that consul residences are sometimes located within the official consular premises. In such cases, only the official office space is protected from police entry.

Dept. of State Law Enforcement Guide to Diplomatic and Consular Immunity

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Rapid Response and Deployment

413.1 PURPOSE AND SCOPE

Violence that is committed in schools, workplaces, public gatherings, and other locations by individuals or a group of individuals who are determined to target and kill persons and to create mass casualties presents a difficult situation for law enforcement. The purpose of this policy is to identify guidelines and factors that will assist deputies in situations that call for rapid response and deployment to such active hostile incidents.

413.1.1 DEFINITIONS

Rapid Response and Deployment - the swift deployment of law enforcement personnel to an active hostile incident where delayed action could result in death or serious bodily injury to innocent people. This is not a substitute for conventional law enforcement response to a barricaded suspect or hostage situation.

Active Hostile Incident – an incident wherein one or more suspects are participating in a random or systematic attack demonstrating their intent to continuously harm others. The object of an active hostile incident appears to be the intent to commit mass casualties/murder. For the purpose of this policy, the term "active hostile incident" includes anyone who uses any other deadly weapon or substance to inflict death or serious bodily injury on multiple victims over a continuous or extended period of time.

413.2 POLICY

The Madison County Sheriff's Office will endeavor to plan for rapid response to crisis situations, and to coordinate response planning with other emergency services as well as with those who are responsible for operating sites that may be the target of a critical incident.

Nothing in this policy shall preclude the use of reasonable force, deadly or otherwise, by members of the Department in protecting themselves or others from death or serious injury.

413.3 CONSIDERATIONS

When dealing with a crisis responding deputies should:

(a) Assess the immediate situation and take reasonable steps to maintain operative control of the incident.

(b) Obtain, explore and analyze sources of intelligence and known information regarding the circumstances, location and suspect involved in the incident.

(c) Attempt to attain a tactical advantage over the suspect by reducing, preventing or eliminating any known or perceived threat.

(d) Attempt, if feasible and based upon the suspect's actions and danger to others, a negotiated surrender of the suspect and release of the hostages.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

413.4 FIRST RESPONSE

If there is a reasonable belief that acts or threats by a suspect are placing lives in imminent danger, first responding deputies should consider reasonable options to reduce, prevent or eliminate the threat. Deputies must decide, often under a multitude of difficult and rapidly evolving circumstances, whether to advance on the suspect, take other actions to deal with the threat or wait for additional resources.

If a suspect is actively engaged in the infliction of serious bodily harm or other life-threatening activity toward others, deputies should take immediate action, if reasonably practicable, while requesting additional assistance.

Deputies should remain aware of the possibility that an incident may be part of a coordinated multi-location attack that may require some capacity to respond to incidents at other locations.

When deciding on a course of action deputies should consider:

(a) Whether to advance on or engage a suspect who is still a possible or perceived threat to others. Any advancement or engagement should be based on information known or received at the time.

(b) Whether to wait for additional resources or personnel.

(c) Whether individuals who are under imminent threat can be moved or evacuated with reasonable safety.

(d) Whether the suspect can be contained or denied access to victims.

(e) Whether the deputies have the ability to effectively communicate with other personnel or resources.

(f) Whether planned tactics can be effectively deployed.

(g) The availability of rifles, shotguns, shields, breaching tools, control devices and any other appropriate tools, and whether the deployment of these tools will provide a tactical advantage.

Absent direction to the contrary, nothingin this policy precludes an individual deputy from taking immediate action when deemed to be reasonable and tactically feasible.

In the case of a barricaded or trapped suspect, with no hostages and no immediate threat to others, deputies should consider covering escape routes and evacuating persons as appropriate, while summoning and waiting for additional assistance (e.g., special tactics and/or hostage negotiation team response).

413.4.1 RAPID EVACUATION AND CONTAINMENT TEAM (REACT)

When the decision is made to advance on or engage a suspect who is still a possible or perceived threat to others is made, deputies should REACT as follows:

The first one to four responding deputies should, where tactically feasible, form a contact team and immediately move toward known suspects or possible locations of known suspects using all

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

available protective equipment to aid in their approach. The most qualified deputy on the scene, regardless of rank, will be the initial contact team leader until such time as they are relieved.

The most senior supervisor on the scene shall be the Incident Commander unless otherwise delegated. The Incident Commander shall evaluate the tactical situation and determine whether additional resources should be summoned, including the Crisis Response Unit (CRU). Refer to the Crisis Response Unit policy for additional guidance.

To the extent that it is tactically feasible, the initial contact team should:

(a) Find the deadly threat

(b) Limit the suspect's movement

(c) Continue past victims to confront active suspects

(d) Communicate progress to other responders, and

(e) Confront the threat through physical control and arrest, containment, or the use of deadly force. Refer to the Use of Force policy for additional guidance.

Subsequent deputies and supervisory personnel who arrive on the scene will REACT as follows:

(a) Assess the tactical situation and assemble additional contact or rescue teams with the following objectives:

1. Approach and enter the location
2. Locate and extract victims to a safe area
3. Notify medical personnel
4. If encountered, as a contact team engage any suspects through control and arrest, containment, or deadly force.

Upon arrival of the Crisis Response Team (CRU), the Incident Commander shall brief the CRU Commander and coordinate with them for:

(a) Assignments and containment responsibilities for suspects

(b) Location, isolation, and neutralization of explosives, if applicable

(c) Gathering of additional intelligence

(d) Assistance with ongoing rescue efforts

(e) Completion of after-action reports

413.5 REPORTS

After the scene has been rendered safe, the Incident Commander shall coordinate the compilation and dissemination of the after-action report concerning all activity during the incident, including any recommendations concerning changes to this policy or procedures. The after-action report shall be forwarded through the chain of command to the Sheriff for review and consideration.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

413.6 PLANNING

The Patrol Division Supervisor should coordinate critical incident planning. Planning efforts should consider:

(a) Identification of likely critical incident target sites, such as schools, shopping centers, entertainment venues and sporting event venues.

(b) Availability of building plans and venue schematics of likely critical incident target sites.

(c) Communications interoperability with other law enforcement and emergency service agencies.

(d) Training opportunities in critical incident target sites, including joint training with site occupants.

(e) Evacuation routes in critical incident target sites.

(f) Patrol first-response training.

(g) Response coordination and resources of emergency medical and fire services.

(h) Equipment needs.

(i) Mutual aid agreements with other agencies.

(j) Coordination with private security providers in critical incident target sites.

413.6.1 SCHOOL CRISIS PLANNING

The Sheriff should annually review the written school crisis, emergency management, and medical emergency response plans as required by Va. Code § 22.1-279.8.

413.7 TRAINING

The Training Supervisor should include rapid response to critical incidents in the training plan. This training should address:

(a) Orientation to likely critical incident target sites, such as schools, shopping centers, entertainment venues and sporting event venues.

(b) Communications interoperability with other law enforcement and emergency service agencies.

(c) Patrol first-response training, including patrol rifle, shotgun, breaching tool and control device training.

(d) First aid, including gunshot trauma.

(e) Reality-based scenario training (e.g., active shooter, disgruntled violent worker).

413.8 SUPPLIES AND EQUIPMENT

The Patrol Division Supervisor should ensure that supplies and equipment required for support of rapid response and deployment events are identified and properly stored in a location and

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

manner to ensure operational readiness. These supplies and equipment should be inspected and inventoried no less than semi-annually and any deficiencies should be promptly resolved.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Immigration Violations

414.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines to members of the Madison County Sheriff's Office relating to immigration and interacting with federal immigration officials.

414.2 POLICY

It is the policy of the Madison County Sheriff's Office that all members make personal and professional commitments to equal enforcement of the law and equal service to the public. Confidence in this commitment will increase the effectiveness of this department in protecting and serving the entire community and recognizing the dignity of all persons, regardless of their national origin or immigration status.

414.3 VICTIMS AND WITNESSES

To encourage crime reporting and cooperation in the investigation of criminal activity, all individuals, regardless of their immigration status, must feel secure that contacting or being addressed by members of law enforcement will not automatically lead to immigration inquiry and/or deportation. While it may be necessary to determine the identity of a victim or witness, members shall treat all individuals equally and not in any way that would violate the United States or Virginia constitutions.

414.3.1 INQUIRING INTO IMMIGRATION STATUS OF VICTIMS OR WITNESSES

No deputy should, in connection with the report, investigation, or prosecution of a crime, inquire into the immigration status of a victim or witness or a parent or guardian of a victim or witness (Va. Code § 19.2-11.02). However, deputies may still inquire into the immigration status of a parent or guardian suspected of committing a crime against a minor victim, as well as enforce or implement the provisions of Va. Code § 18.2-59, Va. Code § 18.2-308.09(10), and Va. Code § 18.2-308.2:2(B1) (Va. Code § 19.2-11.02).

414.4 DETENTIONS

A deputy should not detain any individual, for any length of time, for a civil violation of federal immigration laws or a related civil warrant.

A deputy who has a reasonable suspicion that an individual already lawfully contacted or detained has committed a criminal violation of federal immigration law may detain the person for a reasonable period of time in order to contact federal immigration officials to verify whether an immigration violation is a federal civil violation or a criminal violation. If the violation is a criminal violation, the deputy may continue to detain the person for a reasonable period of time if requested by federal immigration officials (8 USC § 1357(g)(10)). No individual who is otherwise ready to be released should continue to be detained only because questions about the individual’s status are unresolved.

If the deputy has facts that establish probable cause to believe that a person already lawfully detained has committed a criminal immigration offense, he/she may continue the detention and

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

may request a federal immigration official to respond to the location to take custody of the detained person (8 USC § 1357(g)(10)).

A deputy is encouraged to forgo detentions made solely on the basis of a misdemeanor offense when time limitations, availability of personnel, issues of officer safety, communication capabilities, or the potential to obstruct a separate investigation outweigh the need for the detention.

A deputy should notify a supervisor as soon as practicable whenever an individual is being detained for a criminal immigration violation.

414.4.1 PREVIOUSLY DEPORTED FELONS

Deputies lawfully detaining a person discovered to be an alien illegally present in the United States who was deported or left the United States after the felony conviction should notify a supervisor of the circumstances. The supervisor may approve custody under Va. Code § 19.2-81.6 if federal immigration officials verify the person’s presence in the United States qualifies as a federal criminal act and the federal immigration official indicates a federal criminal hold will be sought.

414.4.1 SUPERVISOR RESPONSIBILITIES

When notified that a deputy has detained an individual and established reasonable suspicion or probable cause to believe the person has violated a criminal immigration offense, the supervisor should determine whether it is appropriate to:

(a) Transfer the person to federal authorities.

(b) Lawfully arrest the person for a criminal offense or pursuant to a judicial warrant (see the Law Enforcement Authority Policy).

414.5 ARREST NOTIFICATION TO IMMIGRATION AND CUSTOMS ENFORCEMENT

Generally, a deputy should not notify federal immigration officials when booking arrestees at a jail facility. Any required notification will be handled according to jail operation procedures. No individual who is otherwise ready to be released should continue to be detained solely for the purpose of notification.

414.6 FEDERAL REQUESTS FOR ASSISTANCE

Requests by federal immigration officials for assistance from this department should be directed to a supervisor. The Department may provide available support services, such as traffic control or peacekeeping efforts.

414.7 INFORMATION SHARING

No member of this department will prohibit, or in any way restrict, any other member from doing any of the following regarding the citizenship or immigration status, lawful or unlawful, of any individual (8 USC § 1373):

(a) Sending information to, or requesting or receiving such information from federal immigration officials

(b) Maintaining such information in department records

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) Exchanging such information with any other federal, state, or local government entity

414.7.1 IMMIGRATION DETAINERS

No individual should be held based solely on a federal immigration detainer under 8 CFR 287.7 unless the person has been charged with a federal crime or the detainer is accompanied by a warrant, affidavit of probable cause, or removal order. Notification to the federal authority issuing the detainer should be made prior to the release.

414.8 U VISA AND T VISA NONIMMIGRANT STATUS

Under certain circumstances, federal law allows temporary immigration benefits, known as a U visa, to victims and witnesses of certain qualifying crimes (8 USC § 1101(a)(15)(U)).

Similar immigration protection, known as a T visa, is available for certain qualifying victims of human trafficking (8 USC § 1101(a)(15)(T)).

Any request for assistance in applying for U visa or T visa status should be forwarded in a timely manner to the Investigation Division supervisor assigned to oversee the handling of any related case. The Investigation Division supervisor should:

(a) Consult with the assigned investigator to determine the current status of any related case and whether further documentation is warranted.

(b) Contact the appropriate prosecutor assigned to the case, if applicable, to ensure the certification or declaration has not already been completed and whether a certification or declaration is warranted.

(c) Address the request and complete the certification or declaration, if appropriate, in a timely manner.

1. The instructions for completing certification and declaration forms can be found on the U.S. Department of Homeland Security (DHS) website.

(d) Ensure that any decision to complete, or not complete, a certification or declaration form is documented in the case file and forwarded to the appropriate prosecutor. Include a copy of any completed form in the case file.

414.9 TRAINING

The Training Supervisor should ensure deputies receive training on this policy.

Training should include:

(a) Identifying civil versus criminal immigration violations.

(b) Factors that may be considered in determining whether a criminal immigration offense has been committed.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Utility Service Emergencies

415.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for addressing County utility service emergencies. This policy will address calls for service that are directed to the Sheriff's Department.

415.2 POLICY

It is the policy of the Madison County Sheriff's Office to appropriately respond to County emergency utility service requests received by this department.

415.3 UTILITY SERVICE EMERGENCY

A current contact list of County personnel to be notified in the event of a utility service emergency should be available in the Dispatch Center.

415.3.1 WATER LINES

The County’s responsibility for water lines ends at the water meter; any break or malfunction in the water system from the water meter to a residence or business is the responsibility of the customer.

If a water line break occurs on the County side of the water meter, public works personnel should be notified as soon as practicable.

415.3.2 ELECTRICAL LINES

When a power line poses a hazard, a member of this department should be dispatched to the reported location to protect against personal injury or property damage that might be caused by the power line. The fire department, electric company and/or the public works department should be promptly notified, as appropriate.

415.3.3 RESERVOIRS, PUMPS, WELLS

In the event of flooding or equipment malfunctions involving County reservoirs, pumps or wells, the public works department should be contacted as soon as practicable.

415.3.4 NATURAL GAS LINES

All reports of a possible leak of natural gas or damage to a natural gas line shall promptly be referred to the fire department and the local entity responsible for gas lines. A member of this department should be dispatched to the reported location if it appears that assistance such as traffic control or evacuation is needed.

415.3.5 TRAFFIC SIGNALS

A member of this department should be dispatched upon report of a damaged or malfunctioning traffic signal in order to protect against personal injury or property damage that might occur as the result of the damaged or malfunctioning signal. The member will advise the Dispatch Center of the problem with the traffic signal. The dispatcher should make the necessary notification to the appropriate traffic signal maintenance agency as soon as practicable.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Utility Service Emergencies

A decision to place a signal on flash should include a consultation with the appropriate traffic signal maintenance agency, unless exigent circumstances exist.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Aircraft Accidents

416.1 PURPOSE AND SCOPE

The purpose of this policy is to provide department members with guidelines for handling aircraft accidents.

This policy does not supersede, and is supplementary to, applicable portions of the Crime and Disaster Scene Integrity, Emergency Operations Plan and Hazardous Material Response policies.

416.1.1 DEFINITIONS

Definitions related to this policy include:

Aircraft - Any fixed wing aircraft, rotorcraft, balloon, blimp/dirigible or glider that is capable of carrying a person or any unmanned aerial vehicle other than those intended for non-commercial recreational use.

416.2 POLICY

It is the policy of the Madison County Sheriff's Office to provide an appropriate emergency response to aircraft accidents. This includes emergency medical care and scene management.

416.3 ARRIVAL AT SCENE

Deputies or other authorized members tasked with initial scene management should establish an inner and outer perimeter to:

(a) Protect persons and property.

(b) Prevent any disturbance or further damage to the wreckage or debris, except to preserve life or rescue the injured.

(c) Preserve ground scars and marks made by the aircraft.

(d) Manage the admission and access of public safety and medical personnel to the extent necessary to preserve life or to stabilize hazardous materials.

(e) Maintain a record of persons who enter the accident site.

(f) Consider implementation of an Incident Command System (ICS).

416.4 INJURIES AND CASUALTIES

Members should address emergency medical issues and provide care as a first priority.

Those tasked with the supervision of the scene should coordinate with the Virginia State Police (VSP) and the National Transportation Safety Board (NTSB) before the removal of bodies. If that is not possible, the scene supervisor should ensure documentation of what was disturbed, including switch/control positions and instrument/gauge readings.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

416.5 NOTIFICATIONS

When an aircraft accident is reported to this department, the responding supervisor shall ensure notification is or has been made to NTSB, the Federal Aviation Administration (FAA), the VSP, and when applicable, the appropriate branch of the military.

Supervisors shall ensure other notifications are made once an aircraft accident has been reported. The notifications will vary depending on the type of accident, extent of injuries or damage, and the type of aircraft involved. When an aircraft accident has occurred, it is generally necessary to notify the following:

(a) Fire department

(b) Appropriate airport tower

(c) Emergency medical services (EMS)

416.6 CONTROLLING ACCESS AND SCENE AUTHORITY

Prior to NTSB and VSP arrival, scene access should be limited to authorized personnel from the:

(a) FAA.

(b) Fire department, EMS or other assisting law enforcement agencies.

(c) Medical Examiner.

(d) Air Carrier/Operators investigative teams with NTSB approval.

(e) Appropriate branch of the military, when applicable.

(f) Other emergency services agencies (e.g., hazardous materials teams, biohazard decontamination teams, fuel recovery specialists, explosive ordnance disposal specialists).

The NTSB and the VSP have the primary responsibility for investigating accidents involving civil aircraft. In the case of a military aircraft accident, the appropriate branch of the military will have primary investigation responsibility.

After the NTSB, VSP or military representative arrives on-scene, the efforts of this department will shift to a support role for those agencies.

If NTSB, VSP or a military representative determines that an aircraft or accident does not qualify under its jurisdiction, the on-scene department supervisor should ensure the accident is still appropriately investigated and documented.

416.7 DANGEROUS MATERIALS

Members should be aware of potentially dangerous materials that might be present. These may include, but are not limited to:

- Fuel, chemicals, explosives, biological or radioactive materials and bombs or other ordnance.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

- Pressure vessels, compressed gas bottles, accumulators and tires.
- Fluids, batteries, flares and igniters.
- Evacuation chutes, ballistic parachute systems and composite materials.

416.8 DOCUMENTATION

All aircraft accidents occurring within the County of Madison County, Virginia shall be documented. At a minimum the documentation should include the date, time and location of the incident; any witness statements, if taken; the names of MCSO members deployed to assist; other County resources that were utilized; and cross reference information to other investigating agencies. Suspected criminal activity should be documented on the appropriate crime report.

416.8.1 WRECKAGE

When reasonably safe, members should:

(a) Obtain the aircraft registration number (N number) and note the type of aircraft.

(b) Attempt to ascertain the number of casualties.

(c) Obtain photographs or video of the overall wreckage, including the cockpit and damage, starting at the initial point of impact, if possible, and any ground scars or marks made by the aircraft.

1. Military aircraft may contain classified equipment and therefore shall not be photographed unless authorized by a military commanding officer (18 USC § 795).

(d) Secure, if requested by the lead authority, any electronic data or video recorders from the aircraft that became dislodged or cell phones or other recording devices that are part of the wreckage.

(e) Acquire copies of any recordings from security cameras that may have captured the incident.

416.8.2 WITNESSES

Members tasked with contacting witnesses should obtain:

(a) The location of the witness at the time of his/her observation relative to the accident site.

(b) A detailed description of what was observed or heard.

(c) Any photographs or recordings of the accident witnesses may be willing to voluntarily surrender.

(d) The names of all persons reporting the accident, even if not yet interviewed.

(e) Any audio recordings of reports to 9-1-1 regarding the accident and dispatch records.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

416.9 MEDIA RELATIONS

The Public Information Officer (PIO) should coordinate a response to the media, including access issues, road closures, detours and any safety information that is pertinent to the surrounding community. Any release of information regarding details of the accident itself should be coordinated with the NTSB and VSP or other authority who may have assumed responsibility for the investigation.

Depending on the type of aircraft, the airline or the military may be responsible for family notifications and the release of victims' names. The PIO should coordinate with other involved entities before the release of information.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Field Training

417.1 PURPOSE AND SCOPE

This policy provides guidelines for field training that ensure standardized training and evaluation; facilitate the transition from the academic setting to the actual performance of general law enforcement duties; and introduce the policies, procedures and operations of the Madison County Sheriff's Office. The policy addresses the administration of field training and the selection, supervision, training and responsibilities of the Field Training Officer (FTO).

417.2 POLICY

It is the policy of the Madison County Sheriff's Office that all newly hired or appointed deputy trainees will participate in field training that is staffed and supervised by trained and qualified FTOs.

417.3 FIELD TRAINING

The Department shall establish minimum standards for field training, which should be of sufficient duration to prepare deputy trainees for law enforcement duties and be in compliance with Virginia Department of Criminal Justice Services requirements. The field training is designed to prepare trainees for a patrol assignment and ensure they acquire the skills needed to operate in a safe, productive, and professional manner, in accordance with the general law enforcement duties of this department.

To the extent practicable, field training should include procedures for:

(a) Issuance of training materials to each trainee at the beginning of his/her field training.

(b) Daily and monthly evaluation and documentation of the trainee's performance.

(c) A multiphase structure that includes:

1. A formal evaluation progress report completed by the FTOs involved with the trainee and submitted to the Training Supervisor and FTO coordinator.
2. Assignment of the trainee to a variety of shifts and geographical areas.
3. Assignment of the trainee to a rotation of FTOs in order to provide for an objective evaluation of the trainee's performance.
4. Trainees must complete 3 phases of Field Training
    (a) Phase 1: Observation Phase of minimum 120 hours. Trainee will only ride and observe the FTO.
    (b) Phase 2: Field Training Phase minimum 200 hours. Trainee will carry out tasks with direction and guidance of the FTO.
    (c) Phase 3: Operational Phase minimum 160 hours. Trainee will carry out all tasks with FTO only observing.

(d) The trainee's confidential evaluation of his/her assigned FTOs and the field training process.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(e) Retention of all field training documentation in the deputy trainee's training file including:

1. All performance evaluations.
2. A certificate of completion certifying that the trainee has successfully completed the required number of field training hours.

(f) If trainee does not satisfactorily pass the FTO process then the FTO Coordinator can request up to an additional 160 hours of field training.

See attachment: 417 Field Training Program Completion Record and Competency Attestation.pdf

See attachment: FTO Form.pdf

417.4 FTO COORDINATOR

The Sheriff shall delegate certain responsibilities to an FTO coordinator. The coordinator shall be appointed by and directly responsible to the Patrol Division Supervisor or the authorized designee.

The FTO coordinator may appoint a senior FTO or other designee to assist in the coordination of FTOs and their activities.

The responsibilities of the coordinator include, but are not limited to:

(a) Assignment of trainees to FTOs.

(b) Conducting FTO meetings.

(c) Maintaining and ensuring FTO and trainee performance evaluations are completed.

(d) Maintaining, updating and issuing department training materials to each FTO and trainee.

(e) Developing ongoing training for FTOs.

(f) Mentoring and supervising individual FTO performance.

(g) Monitoring the overall performance of field training.

(h) Keeping the Shift Supervisor informed through monthly evaluation reports about the trainees' progress.

(i) Maintaining a liaison with FTO coordinators from other law enforcement agencies.

(j) Maintaining a liaison with sheriff's academy staff on recruit deputy performance during academy attendance.

(k) Performing other activities as may be directed by the Patrol Division Supervisor.

The FTO coordinator will be required to successfully complete a training course approved by this department that is applicable to supervision of field training within one year of appointment to this position.

417.5 FTO SELECTION, TRAINING AND RESPONSIBILITIES

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Field Training

417.5.1 SELECTION PROCESS

The selection of an FTO will be at the discretion of the Sheriff or the authorized designee. Selection will be based on the deputy's:

(a) Desire to be an FTO.

(b) Completion of the probationary period.

(c) Demonstrated ability as a positive role model.

(d) Evaluation by supervisors and current FTOs.

(e) Possession of, or ability to obtain, department-approved certification.

An FTO must remain in good standing and may be relieved from FTO duties by the Sheriff due to discipline, inappropriate conduct or poor performance.

417.5.2 TRAINING

A deputy selected as an FTO shall successfully complete the minimum training standards established by the Department of Criminal Justice Services prior to being assigned as an FTO (6 VAC 20-280-20).

All FTOs must complete an FTO update course approved by this department every three years while assigned to the position of FTO (6 VAC 20-280-70).

417.5.3 TRAINING MATERIALS

The FTO shall receive training materials outlining the requirements, expectations and objectives of the FTO position. FTOs should refer to their training materials or the FTO coordinator regarding specific questions related to FTO or field training.

417.5.4 PROVISIONAL FIELD TRAINING OFFICER

If a situation arises where the Department does not have a deputy who has completed the minimum training requirements for an FTO, the Department may temporarily provide field training with a deputy who has been certified as a provisional FTO by the Department of Criminal Justice Services until a fully trained FTO is available (6 VAC 20-280-30).

417.5.5 RESPONSIBILITIES

The responsibilities of the FTO include, but are not limited to:

(a) Issuing his/her assigned trainee field training materials in accordance with the Training Policy.

1. The FTO shall ensure that the trainee has the opportunity to become knowledgeable of the subject matter and proficient with the skills as set forth in the training materials.
2. The FTO shall sign off on all completed topics contained in the training materials, noting the methods of learning and evaluating the performance of his/her assigned trainee.

(b) Completing and reviewing daily performance evaluations with the trainee.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) Completing and submitting a written evaluation on the performance of his/her assigned trainee to the FTO coordinator on a daily basis.

(d) Completing a detailed weekly performance evaluation of his/her assigned trainee at the end of each week.

(e) Completing a monthly evaluation report of his/her assigned trainee at the end of each month.

(f) Providing the shift supervisor with a verbal synopsis of the trainee's activities at the end of each day or during any unusual occurrence needing guidance or clarification upon request.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Air Support

418.1 PURPOSE AND SCOPE

The use of air support can be invaluable in certain situations. This policy specifies situations where the use of air support may be requested and the responsibilities for making a request.

418.2 POLICY

It is the policy of the Madison County Sheriff's Office to prioritize requests for air support to enhance law enforcement objectives and provide additional safety to deputies and the community.

418.3 REQUEST FOR AIR SUPPORT

If a supervisor or deputy in charge of an incident determines that the use of air support would be beneficial, a request to obtain air support may be made to the Sheriff.

418.3.1 CIRCUMSTANCES FOR REQUESTS

Law enforcement air support may be requested under conditions that include, but are not limited to:

(a) When the safety of deputies or the community is in jeopardy and the presence of air support may reduce such hazard.

(b) When the use of air support will aid in the capture of a suspected fleeing felon whose continued freedom represents an ongoing threat to deputies or the community.

(c) When air support is needed to locate a person who is lost and whose continued absence constitutes a serious health or safety hazard.

(d) Vehicle pursuits.

(e) Pre-planned events or actions that require air support.

(f) Due to a request under an existing mutual aid agreement.

(g) When the Shift Supervisor or equivalent authority determines a reasonable need exists.

418.3.2 ALLIED AGENCY REQUEST

After consideration and approval of the request for air support, the Sheriff will call the Virginia State Police or, in the case where VSP air support is not available, the closest agency having available air support and will apprise that agency of the specific details of the incident prompting the request.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Contacts and Temporary Detentions

419.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for temporarily detaining but not arresting persons in the field, conducting field interviews (FI) and pat-down searches, and the taking and disposition of photographs.

419.1.1 DEFINITIONS

Definitions related to this policy include:

Consensual encounter - When a deputy contacts an individual but does not create a detention through words, actions, or other means. In other words, a reasonable individual would believe that his/her contact with the deputy is voluntary.

Field interview (FI) - The brief detainment of an individual, whether on foot or in a vehicle, based on reasonable suspicion for the purpose of determining the individual's identity and resolving the deputy's suspicions.

Field photographs - Posed photographs taken of a person during a contact, temporary detention, or arrest in the field. Undercover surveillance photographs of an individual and recordings captured by the normal operation of a Mobile Audio/Video (MAV) system, body-worn camera, or public safety camera when persons are not posed for the purpose of photographing are not considered field photographs.

Pat-down search - A type of search used by deputies in the field to check an individual for dangerous weapons. It involves a thorough patting-down of clothing to locate any weapons or dangerous items that could pose a danger to the deputy, the detainee, or others.

Reasonable suspicion - When, under the totality of the circumstances, a deputy has articulable facts that criminal activity may be afoot and a particular person is connected with that possible criminal activity.

Temporary detention - When a deputy intentionally, through words, actions, or physical force, causes an individual to reasonably believe he/she is required to restrict his/her movement without an actual arrest. Temporary detentions also occur when a deputy actually restrains a person’s freedom of movement.

419.2 POLICY

The Madison County Sheriff's Office respects the right of the public to be free from unreasonable searches or seizures. Due to an unlimited variety of situations confronting the deputy, the decision to temporarily detain a person and complete an FI, pat-down search or field photograph shall be left to the deputy based on the totality of the circumstances, officer safety considerations and constitutional safeguards.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

419.3 FIELD INTERVIEWS

Based on observance of suspicious circumstances or upon information from investigation, a deputy may initiate the stop of a person, and conduct an FI, when there is articulable, reasonable suspicion to do so. A person, however, shall not be detained longer than is reasonably necessary to resolve the deputy's suspicion.

Nothing in this policy is intended to discourage consensual contacts. Frequent casual contact with consenting individuals is encouraged by the Madison County Sheriff's Office to strengthen community involvement, community awareness and problem identification.

419.3.1 INITIATING A FIELD INTERVIEW

When initiating the stop, the deputy should be able to point to specific facts which, when considered with the totality of the circumstances, reasonably warrant the stop. Such facts include but are not limited to an individual's:

(a) Appearance or demeanor suggesting that he/she is part of a criminal enterprise or is engaged in a criminal act.

(b) Actions suggesting that he/she is engaged in a criminal activity.

(c) Presence in an area at an inappropriate hour of the day or night.

(d) Presence in a particular area is suspicious.

(e) Carrying of suspicious objects or items.

(f) Excessive clothes for the climate or clothes bulging in a manner that suggest he/she is carrying a dangerous weapon.

(g) Location in proximate time and place to an alleged crime.

(h) Physical description or clothing worn that matches a suspect in a recent crime.

(i) Prior criminal record or involvement in criminal activity as known by the deputy.

419.4 PAT-DOWN SEARCHES

Once a valid stop has been made, and consistent with the deputy's training and experience, a deputy may pat a suspect's outer clothing for weapons if the deputy has a reasonable, articulable suspicion the suspect may pose a safety risk. The purpose of this limited search is not to discover evidence of a crime, but to allow the deputy to pursue the investigation without fear of violence. Circumstances that may establish justification for performing a pat-down search include but are not limited to:

(a) The type of crime suspected, particularly in crimes of violence where the use or threat of weapons is involved.

(b) Where more than one suspect must be handled by a single deputy.

(c) The hour of the day and the location or area where the stop takes place.

(d) Prior knowledge of the suspect's use of force and/or propensity to carry weapons.

(e) The actions and demeanor of the suspect.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(f) Visual indications which suggest that the suspect is carrying a firearm or other dangerous weapon.

Whenever practicable, a pat-down search should not be conducted by a lone deputy. A cover deputy should be positioned to ensure safety and should not be involved in the search.

419.5 FIELD PHOTOGRAPHS

All available databases should be searched before photographing any field detainee. If a photograph is not located, or if an existing photograph no longer resembles the detainee, the deputy shall carefully consider, among other things, the factors listed below.

419.5.1 FIELD PHOTOGRAPHS TAKEN WITH CONSENT

Field photographs may be taken when the subject being photographed knowingly and voluntarily gives consent. When taking a consensual photograph, the deputy should have the individual read and sign the appropriate form accompanying the photograph.

419.5.2 FIELD PHOTOGRAPHS TAKEN WITHOUT CONSENT

Field photographs may be taken without consent only if they are taken during a detention that is based upon reasonable suspicion of criminal activity, and the photograph serves a legitimate law enforcement purpose related to the detention. The deputy must be able to articulate facts that reasonably indicate that the subject was involved in or was about to become involved in criminal conduct. The subject should not be ordered to remove or lift any clothing for the purpose of taking a photograph.

If, prior to taking a photograph, the deputy's reasonable suspicion of criminal activity has been dispelled, the detention must cease and the photograph should not be taken.

All field photographs and related reports shall be submitted to a supervisor and retained in compliance with this policy.

419.5.3 DISPOSITION OF PHOTOGRAPHS

All detainee photographs must be adequately labeled and submitted to the Shift Supervisor with documentation explaining the nature of the contact. If an individual is photographed as a suspect in a particular crime, the photograph should be submitted as an evidence item in the related case, following standard evidence procedures.

If a photograph is not associated with an investigation where a case number has been issued, the Shift Supervisor should review and forward the photograph to one of the following locations:

(a) If the photograph and associated FI or documentation is relevant to criminal organization/enterprise enforcement, the Shift Supervisor will forward the photograph and documents to the designated criminal intelligence system supervisor. The supervisor will ensure the photograph and supporting documents are retained as prescribed in the Criminal Organizations Policy.

(b) Photographs that do not qualify for retention in a criminal intelligence system or temporary information file shall be forwarded to the Records Division.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

When a photograph is taken in association with a particular case, the investigator may use such photograph in a photo lineup. Thereafter, the individual photograph should be retained as a part of the case file. All other photographs shall be retained in accordance with the established records retention schedule.

419.5.4 SUPERVISOR RESPONSIBILITIES

While it is recognized that field photographs often become valuable investigative tools, supervisors should monitor such practices in view of the above listed considerations. This is not to imply that supervisor approval is required before each photograph is taken.

Access to, and use of, field photographs shall be strictly limited to law enforcement purposes.

419.6 WITNESS IDENTIFICATION AND INTERVIEWS

Because potential witnesses to an incident may become unavailable or the integrity of their statements compromised with the passage of time, deputies should, when warranted by the seriousness of the case, take reasonable steps to promptly coordinate with an on-scene supervisor and/or criminal investigator to utilize available members for the following:

(a) Identifying all persons present at the scene and in the immediate area.

1. When feasible, a recorded statement should be obtained from those who claim not to have witnessed the incident but who were present at the time it occurred.
2. Any potential witness who is unwilling or unable to remain available for a formal interview should not be detained absent reasonable suspicion to detain or probable cause to arrest. Without detaining the individual for the sole purpose of identification, deputies should attempt to identify the witness prior to his/her departure.

(b) Witnesses who are willing to provide a formal interview should be asked to meet at a suitable location where criminal investigators may obtain a recorded statement. Such witnesses, if willing, may be transported by department members.

1. A written, verbal or recorded statement of consent should be obtained prior to transporting a witness. When the witness is a minor, consent should be obtained from the parent or guardian, if available, prior to transport.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Criminal Organizations

420.1 PURPOSE AND SCOPE

The purpose of this policy is to ensure that the Madison County Sheriff's Office appropriately utilizes criminal intelligence systems and temporary information files to support investigations of criminal organizations and enterprises.

420.1.1 DEFINITIONS

Definitions related to this policy include:

Criminal intelligence system - Any record system that receives, stores, exchanges or disseminates information that has been evaluated and determined to be relevant to the identification of a criminal organization or enterprise, its members or affiliates. This does not include temporary information files.

420.2 POLICY

The Madison County Sheriff's Office recognizes that certain criminal activities, including, but not limited to gang crimes and drug trafficking, often involve some degree of regular coordination and may involve a large number of participants over a broad geographical area.

It is the policy of this department to collect and share relevant information while respecting the privacy and legal rights of the public.

420.3 CRIMINAL INTELLIGENCE SYSTEMS

No department member may create, submit to or obtain information from a criminal intelligence system unless the Sheriff has approved the system for department use.

Any criminal intelligence system approved for department use should meet or exceed the standards of 28 CFR 23.20.

A designated supervisor will be responsible for maintaining each criminal intelligence system that has been approved for department use. The supervisor or the authorized designee should ensure the following:

(a) Members using any such system are appropriately selected and trained.

(b) Use of every criminal intelligence system is appropriately reviewed and audited.

(c) Any system security issues are reasonably addressed.

Madison County Sheriff's Office Law Enforcement Procedures Manual: 405.1 Criminal Intelligence Systems Operating Principles (28 CFR 23.20)

420.3.1 SYSTEM ENTRIES

It is the designated supervisor’s responsibility to approve the entry of any information from a report, field interview (FI), photo or other relevant document into an authorized criminal intelligence system. If entries are made based upon information that is not on file with this department, such as open or public source documents or documents that are on file at another agency, the designated

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

supervisor should ensure copies of those documents are retained by the Records Division. Any supporting documentation for an entry shall be retained by the Records Division in accordance with the established records retention schedule and for at least as long as the entry is maintained in the system.

The designated supervisor should ensure that any documents retained by the Records Division are appropriately marked as intelligence information. The Records Manager may not purge such documents without the approval of the designated supervisor.

420.4 TEMPORARY INFORMATION FILE

No member may create or keep files on individuals that are separate from the approved criminal intelligence system. However, members may maintain temporary information that is necessary to actively investigate whether a person or group qualifies for entry into the department-approved criminal intelligence system only as provided in this section. Once information qualifies for inclusion, it should be submitted to the supervisor responsible for consideration of criminal intelligence system entries.

420.4.1 FILE CONTENTS

A temporary information file may only contain information and documents that, within one year, will have a reasonable likelihood to meet the criteria for entry into an authorized criminal intelligence system.

Information and documents contained in a temporary information file:

(a) Must only be included upon documented authorization of the responsible department supervisor.

(b) Should not be originals that would ordinarily be retained by the Records Division or Property and Evidence Section, but should be copies of, or references to, retained documents, such as copies of reports, FI forms, the Dispatch Center records or booking forms.

(c) Shall not include opinions. No person, organization or enterprise shall be labeled as being involved in crime beyond what is already in the document or information.

(d) May include information collected from publicly available sources or references to documents on file with another government agency. Attribution identifying the source should be retained with the information.

420.4.2 FILE REVIEW AND PURGING

The contents of a temporary information file shall not be retained longer than one year. At the end of one year, the contents must be purged.

The designated supervisor shall periodically review the temporary information files to verify that the contents meet the criteria for retention. Validation and purging of files is the responsibility of the supervisor.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

420.5 INFORMATION RECOGNITION

Department members should document facts that suggest an individual, organization or enterprise is involved in criminal activity and should forward that information appropriately. Examples include, but are not limited to:

(a) Gang indicia associated with a person or residence.

(b) Information related to a drug-trafficking operation.

(c) Vandalism indicating an animus for a particular group.

(d) Information related to an illegal gambling operation.

Department supervisors who utilize an authorized criminal intelligence system should work with the Training Supervisor to train members to identify information that may be particularly relevant for inclusion.

420.6 RELEASE OF INFORMATION

Department members shall comply with the rules of an authorized criminal intelligence system regarding inquiries and release of information.

Information from a temporary information file may only be furnished to department members and other law enforcement agencies on a need-to-know basis and consistent with the Records Maintenance and Release Policy.

When an inquiry is made by the parent or guardian of a juvenile as to whether that juvenile's name is in a temporary information file, such information should be provided by the supervisor responsible for the temporary information file, unless there is good cause to believe that the release of such information might jeopardize an ongoing criminal investigation.

420.7 CRIMINAL STREET GANGS

The Investigation Division supervisor should ensure that there are an appropriate number of department members who can:

(a) Testify as experts on matters related to criminal street gangs, and maintain an above-average familiarity with criminal street gang activities, membership and predicate criminal street gang crimes (Va. Code § 18.2-46.1).

(b) Coordinate with other agencies in the region regarding criminal street gang-related crimes and information.

(c) Train other members to identify gang indicia and investigate criminal street gang-related crimes.

420.8 REPORTS TO THE SHERIFF

The Investigation Division Supervisor should complete and submit a monthly report to the Sheriff regarding investigative reports and activities involving vice, drugs and organized crimes. The Investigation Division Supervisor should periodically brief the Sheriff regarding sensitive investigations involving vice, drugs, organized crimes and other major criminal activities.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

420.9 TRAINING

The Training Supervisor should provide training on best practices in the use of each authorized criminal intelligence system to those tasked with investigating criminal organizations and enterprises. Training should include:

(a) The protection of civil liberties.

(b) Participation in a multi-agency criminal intelligence system.

(c) Submission of information into a multi-agency criminal intelligence system or the receipt of information from such a system, including any governing federal and state rules and statutes.

(d) The type of information appropriate for entry into a criminal intelligence system or temporary information file.

(e) The review and purging of temporary information files.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Shift Supervisors

421.1 PURPOSE AND SCOPE

This policy provides guidelines for the designation of a Shift Supervisor and, as needed, an acting Shift Supervisor for each shift.

421.2 POLICY

Each shift will be directed by a Shift Supervisor capable of making decisions and managing in a manner consistent with the mission of the Madison County Sheriff's Office. To accomplish this, a First Sergeant shall be designated as the Shift Supervisor for each shift.

421.3 DESIGNATION AS ACTING SHIFT SUPERVISOR

With prior authorization from the Patrol Division Supervisor, generally when a First Sergeant is unavailable for duty as Shift Supervisor, a qualified lower-ranking member shall be designated as acting Shift Supervisor in accordance with the terms of applicable county rule or policy and the Temporary Supervisors subsection of the Supervision Staffing Levels Policy.

421.4 SHIFT SUPERVISOR RESPONSIBILITIES

The Shift Supervisor shall have overall responsibility and accountability for the operation of this department on an assigned shift. Duties may include, but are not limited to:

(a) Ensuring at least one uniformed patrol supervisor is deployed during each shift, in addition to the Shift Supervisor.

(b) Ensuring sufficient members are on-duty to accomplish the mission of the Madison County Sheriff's Office.

(c) Providing command-level oversight of major crime scenes, tactical situations, or disasters.

(d) Establishing service-level priorities.

(e) Providing job-related training and guidance to subordinates.

(f) Acquiring outside resources or providing assistance to other agencies, when applicable.

(g) Handling service inquiries or complaints from the public.

(h) Managing risk exposure.

(i) Ensuring the security of all department facilities.

(j) Ensuring the proper equipment and vehicles are available for member use.

(k) Representing the Department at community functions.

(l) Serving as a temporary Division Supervisor when so designated.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Mobile Audio/Video

422.1 PURPOSE AND SCOPE

The Madison County Sheriff's Office has equipped marked law enforcement vehicles with Mobile Audio/Video (MAV) recording systems to provide records of events and to assist deputies in the performance of their duties. This policy provides guidance on the use of these systems.

422.1.1 DEFINITIONS

Definitions related to this policy include:

Activate - Any process that causes the MAV system to transmit or store video or audio data in an active mode.

In-car camera system and MAV system - Synonymous terms that refer to any system that captures audio and video signals, that is capable of installation in a vehicle, and that includes at a minimum, a camera, microphone, recorder and monitor.

MAV technician - Personnel certified or trained in the operational use and repair of MAVs, duplicating methods and storage and retrieval methods and who have a working knowledge of video forensics and evidentiary procedures.

Recorded media - Audio/video signals recorded or digitally stored on a storage device or portable media.

422.2 POLICY

It is the policy of the Madison County Sheriff's Office to use mobile audio/video technology to more effectively fulfill the mission of the Department and to ensure these systems are used securely and efficiently.

422.3 DEPUTY RESPONSIBILITIES

Prior to going into service, each deputy will properly equip him/herself to record audio and video in the field. At the end of the shift, each deputy will follow the established procedures for providing to the Department any recordings or used media and any other related equipment. Each deputy should have adequate recording media for the entire duty assignment. In the event a deputy works at a remote location and reports in only periodically, additional recording media may be issued. Only Madison County Sheriff's Office identified and labeled media with tracking numbers is to be used.

At the start of each shift, deputies should test the MAV system’s operation in accordance with manufacturer specifications and department operating procedures and training.

System documentation is accomplished by the deputy recording his/her name, serial number, badge or personal identification number (PIN) and the current date and time at the start and again at the end of each shift. If the system is malfunctioning, the deputy shall take the vehicle out of service unless a supervisor requests the vehicle remain in service.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

422.4 ACTIVATION OF THE MAV

The MAV system is designed to turn on whenever the vehicle's emergency lights are activated. The system remains on until it is turned off manually. The audio portion is independently controlled and should be activated manually by the deputy whenever appropriate. When audio is being recorded, the video will also record.

422.4.1 REQUIRED ACTIVATION OF THE MAV

This policy is not intended to describe every possible situation in which the MAV system may be used, although there are many situations where its use is appropriate. A deputy may activate the system any time the deputy believes it would be appropriate or valuable to document an incident.

In some circumstances it is not possible to capture images of the incident due to conditions or the location of the camera. However, the audio portion can be valuable evidence and is subject to the same activation requirements as the MAV. The MAV system should be activated in any of the following situations:

(a) All field contacts involving actual or potential criminal conduct within video or audio range:

1. Traffic stops (including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops)
2. Priority responses
3. Vehicle pursuits
4. Suspicious vehicles
5. Arrests
6. Vehicle searches
7. Physical or verbal confrontations or use of force
8. Pedestrian checks
9. Driving while under the influence (DUI) investigations, including field sobriety tests
10. Consensual encounters
11. Crimes in progress
12. Responding to an in-progress call

(b) All self-initiated activity in which a deputy would normally notify the Dispatch Center

(c) Any call for service involving a crime where the recorder may aid in the apprehension and/or prosecution of a suspect, including:

1. Domestic or family violence
2. Disturbance of the peace

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

3. Offenses involving violence or weapons

(d) Any other contact that becomes adversarial after the initial contact, in a situation that would not otherwise require recording

(e) Any other circumstance where the deputy believes that a recording of an incident would be appropriate

Activation of the MAV system is not required when exchanging information with other deputies, during breaks or lunch periods, or when not in service or not actively on patrol.

422.4.2 CESSATION OF RECORDING

Once activated, the MAV system should remain on until the incident has concluded. For the purpose of this section, conclusion of an incident has occurred when all arrests have been made, arrestees have been transported and all witnesses and victims have been interviewed. Recording may cease if a deputy is simply waiting for a tow truck or a family member to arrive, or in other similar situations.

422.4.3 SURREPTITIOUS RECORDING

No member of this department may surreptitiously record a conversation of any other member of this department except with a court order or when lawfully authorized by the Sheriff or the authorized designee for the purpose of conducting a criminal or administrative investigation.

422.4.4 SUPERVISOR RESPONSIBILITIES

Supervisors should determine if vehicles with non-functioning MAV systems should be placed into service. If these vehicles are placed into service, the appropriate documentation should be made, including notification of the Dispatch Center.

At reasonable intervals, supervisors should validate that:

(a) Beginning and end-of-shift recording procedures are followed.

(b) Logs reflect the proper chain of custody, including:

1. The tracking number of the MAV system media.
2. The date the media was issued.
3. The name of the department member or the vehicle to which the media was issued.
4. The date the media was submitted for retention.
5. The name of the department member submitting the media.
6. Holds for evidence indication and tagging as required.

(c) The operation of MAV systems by new members is assessed and reviewed no less than biweekly.

When an incident arises that requires the immediate retrieval of the recorded media (e.g., serious crime scenes, officer-involved shootings, department-involved traffic accidents), a supervisor shall

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

respond to the scene and ensure that the appropriate person properly retrieves the recorded media. The media may need to be treated as evidence and should be handled in accordance with current evidence procedures for recorded media.

Supervisors may activate the MAV system remotely to monitor a developing situation, such as a chase, riot or an event that may threaten public safety, officer safety or both, when the purpose is to obtain tactical information to assist in managing the event. Supervisors shall not remotely activate the MAV system for the purpose of monitoring the conversations or actions of a deputy.

422.5 REVIEW OF MAV RECORDINGS

All recording media, recorded images and audio recordings are the property of the Department. Dissemination outside of the Department is strictly prohibited, except to the extent permitted or required by law.

To prevent damage to, or alteration of, the original recorded media, it shall not be copied, viewed or otherwise inserted into any device not approved by the Department, MAV technician or forensic media staff. When reasonably possible, a copy of the original media shall be used for viewing (unless otherwise directed by the courts) to preserve the original media.

Recordings may be reviewed in any of the following situations:

(a) By deputies for use when preparing reports or statements

(b) By a supervisor investigating a specific act of deputy conduct

(c) By a supervisor to assess deputy performance

(d) To assess proper functioning of MAV systems

(e) By department investigators who are participating in an official investigation, such as a personnel complaint, administrative inquiry or a criminal investigation

(f) By department personnel who request to review recordings

(g) By a deputy who is captured on or referenced in the video or audio data, and reviews and uses such data for any purpose relating to his/her employment

(h) By court personnel through proper process or with the permission of the Sheriff or the authorized designee

(i) By the media through proper process

(j) To assess possible training value

(k) For training purposes. If an involved deputy objects to showing a recording, his/her objection will be submitted to the command staff to determine if the training value outweighs the deputy's objection.

(l) As may be directed by the Sheriff or the authorized designee

Members desiring to view any previously uploaded or archived MAV recording should submit a request in writing to the Shift Supervisor. Approved requests should be forwarded to the MAV technician for processing.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

In no event shall any recording be used or shown for the purpose of ridiculing or embarrassing any member.

422.5.1 RELEASE OF RECORDINGS
Requests for the release of audio/video recordings shall be processed in accordance with the Records Maintenance and Release Policy.

422.6 DOCUMENTING MAV USE

If any incident is recorded with either the video or audio system, the existence of that recording shall be documented in the deputy's report. If a citation is issued, the deputy shall make a notation on the back of the records copy of the citation indicating that the incident was recorded.

422.7 RECORDING MEDIA STORAGE AND INTEGRITY

Once submitted for storage, all recording media will be labeled and stored in a designated secure area. All recording media that is not booked as evidence will be retained for a minimum of 30 days and disposed of in accordance with the established records retention schedule (Va. Code § 42.1-76 et seq.).

422.7.1 COPIES OF ORIGINAL RECORDING MEDIA
Original recording media shall not be used for any purpose other than for initial review by a supervisor. Upon proper request, a copy of the original recording media will be made for use as authorized in this policy.

Original recording media may only be released in response to a court order or upon approval by the Sheriff or the authorized designee. In the event that an original recording is released to a court, a copy shall be made and placed in storage until the original is returned.

422.7.2 MAV RECORDINGS AS EVIDENCE
Deputies who reasonably believe that a MAV recording is likely to contain evidence relevant to a criminal offense or to a potential claim against the deputy or against the Madison County Sheriff's Office should indicate this in an appropriate report. Deputies should ensure relevant recordings are preserved.

422.8 SYSTEM OPERATIONAL STANDARDS

(a) MAV system vehicle installations should be based on officer safety requirements and the vehicle and device manufacturer’s recommendations.

(b) The MAV system should be configured to minimally record for 30 seconds prior to an event.

(c) The MAV system may not be configured to record audio data occurring prior to activation.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Unless the transmitters being used are designed for synchronized use, only one transmitter, usually the primary initiating deputy's transmitter, should be activated at a scene to minimize interference or noise from other MAV transmitters.

(e) Deputies using digital transmitters that are synchronized to their individual MAVs shall activate both audio and video recordings when responding in a support capacity. This is to obtain additional perspectives of the incident scene.

(f) With the exception of law enforcement radios or other emergency equipment, other electronic devices should not be used inside MAV-equipped law enforcement vehicles to minimize the possibility of causing electronic or noise interference with the MAV system.

(g) Deputies shall not erase, alter, reuse, modify or tamper with MAV recordings. Only a supervisor, MAV technician or other authorized designee may erase and reissue previous recordings and may only do so pursuant to the provisions of this policy.

422.9 MAV TECHNICIAN RESPONSIBILITIES

The MAV technician is responsible for:

(a) Ordering, issuing, retrieving, storing, erasing and duplicating of all recorded media.

(b) Collecting all completed media for oversight and verification of wireless downloaded media. Once collected, the MAV technician:

1. Ensures it is stored in a secure location with authorized controlled access.
2. Makes the appropriate entries in the chain of custody log.

(c) Erasing of media:

1. Pursuant to a court order.
2. In accordance with the established records retention schedule, including reissuing all other media deemed to be of no evidentiary value.

(d) Assigning all media an identification number prior to issuance to the field:

1. Maintaining a record of issued media.

(e) Ensuring that an adequate supply of recording media is available.

(f) Managing the long-term storage of media that has been deemed to be of evidentiary value in accordance with the department evidence storage protocols and the established records retention schedule.

422.10 TRAINING

All members who are authorized to use the MAV system shall successfully complete an approved course of instruction prior to its use.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Mobile Data Computer Use

423.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the proper access, use and application of the Mobile Data Computer (MDT) system in order to ensure proper access to confidential records from local, state and national law enforcement databases, and to ensure effective electronic communications between department members and the Dispatch Center.

423.2 POLICY

Madison County Sheriff's Office members using the MDT shall comply with all appropriate federal and state rules and regulations and shall use the MDT in a professional manner, in accordance with this policy.

423.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to messages accessed, transmitted, received or reviewed on any department technology system (see the Information Technology Use Policy for additional guidance).

423.4 RESTRICTED ACCESS AND USE

MDT use is subject to the Information Technology Use and Protected Information policies.

Members shall not access the MDT system if they have not received prior authorization and the required training. Members shall immediately report unauthorized access or use of the MDT by another member to their Shift Supervisor, or Division Supervisor

Use of the MDT system to access law enforcement databases or transmit messages is restricted to official activities, business-related tasks, or communications that are directly related to the business, administration or practices of the Department. In the event that a member has questions about sending a particular message or accessing a particular database, the member should seek prior approval from his/her supervisor.

Sending derogatory, defamatory, obscene, disrespectful, sexually suggestive, harassing or any other inappropriate messages on the MDT system is prohibited and may result in discipline.

It is a violation of this policy to transmit a message or access a law enforcement database under another member's name or to use the password of another member to log in to the MDT system unless directed to do so by a supervisor. Members are required to log off the MDT or secure the MDT when it is unattended. This added security measure will minimize the potential for unauthorized access or misuse.

423.4.1 USE WHILE DRIVING

Use of the MDT by the vehicle operator should generally be limited to times when the vehicle is stopped. When the vehicle is in motion, the operator should only attempt to read messages that are likely to contain information that is required for immediate enforcement, investigative or safety needs.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Short transmissions, such as a license plate check, are permitted if it reasonably appears that it can be done safely. In no case shall an operator attempt to send or review lengthy messages while the vehicle is in motion.

423.5 DOCUMENTATION OF ACTIVITY

Except as otherwise directed by the Shift Supervisor or other department-established protocol, all calls for service assigned by a dispatcher should be communicated by voice over the sheriff's radio and electronically via the MDT unless security or confidentiality prevents such broadcasting.

MDT and voice transmissions are used to document the member's daily activity. To ensure accuracy:

(a) All contacts or activity shall be documented at the time of the contact.

(b) Whenever the activity or contact is initiated by voice, it should be documented by a dispatcher.

(c) Whenever the activity or contact is not initiated by voice, the member shall document it via the MDT.

423.5.1 STATUS CHANGES

All changes in status (e.g., arrival at scene, meal periods, in service) will be transmitted over the sheriff's radio or through the MDT system.

Members responding to in-progress calls should advise changes in status over the radio to assist other members responding to the same incident. Other changes in status can be made on the MDT.

423.5.2 EMERGENCY ACTIVATION

If there is an emergency activation and the member does not respond to a request for confirmation of the need for emergency assistance or confirms the need, available resources will be sent to assist in locating the member. If the location is known, the nearest available deputy should respond in accordance with the Deputy Response to Calls Policy.

Members should ensure a field supervisor and the Shift Supervisor are notified of the incident without delay.

Deputies not responding to the emergency shall refrain from transmitting on the sheriff's radio until a no-further-assistance broadcast is made or if they are handling a different emergency.

423.6 EQUIPMENT CONSIDERATIONS

423.6.1 MALFUNCTIONING MDT

Whenever possible, members will not use malfunctioning MDTs. Whenever members MDT is not working, they shall notify the Dispatch Center. It shall be the responsibility of the dispatcher to document all information that will then be transmitted verbally over the sheriff's radio.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

423.6.2 BOMB CALLS

When investigating reports of possible bombs, members should not communicate on their MDTs when in the evacuation area of a suspected explosive device. Radio frequency emitted by the MDT could cause some devices to detonate.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Portable Audio/Video Recorders

424.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of portable audio/video recording devices by members of this department while in the performance of their duties. Portable audio/video recording devices include all recording systems whether body-worn, hand-held, or integrated into portable equipment.

This policy does not apply to mobile audio/video recordings, interviews, or interrogations conducted at any Madison County Sheriff's Office facility, authorized undercover operations, wiretaps, or eavesdropping (concealed listening devices).

This policy provides guidelines consistent with Va. Code § 15.2-1723.1 which requires the adoption of a policy before a body-worn recording system may be purchased or deployed.

424.2 POLICY

The Madison County Sheriff's Office may provide members with access to portable recorders, either audio or video or both, for use during the performance of their duties. The use of recorders is intended to enhance the mission of the Department by accurately capturing contacts between members of the Department and the public.

424.3 COORDINATOR

The Sheriff or the authorized designee should designate a coordinator responsible for:

(a) Establishing procedures for the security, storage and maintenance of data and recordings.

(b) Establishing procedures for accessing data and recordings.

(c) Establishing procedures for logging or auditing access.

(d) Establishing procedures for transferring, downloading, tagging or marking events.

424.4 MEMBER PRIVACY EXPECTATION

All recordings made by members on any department-issued device at any time, and any recording made while acting in an official capacity of this department, regardless of ownership of the device it was made on, shall remain the property of the Department. Members shall have no expectation of privacy or ownership interest in the content of these recordings.

424.5 MEMBER RESPONSIBILITIES

Prior to going into service, each uniformed member will be responsible for making sure that he/she is equipped with a portable recorder, issued by the Department, and that the recorder is in good working order. If the recorder is not in working order or the member becomes aware of a malfunction at any time, the member shall promptly report the failure to his/her supervisor and obtain a functioning device as soon as reasonably practicable. Uniformed members should wear the recorder in a conspicuous manner or otherwise notify persons that they are being recorded, whenever reasonably practicable.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Any member assigned to a non-uniformed position may carry an approved portable recorder at any time the member believes that such a device may be useful. Unless conducting a lawful recording in an authorized undercover capacity, non-uniformed members should wear the recorder in a conspicuous manner when in use or otherwise notify persons that they are being recorded, whenever reasonably practicable.

When using a recorder, the assigned member shall record his/her name, MCSO identification number and the current date and time at the beginning and the end of the shift or other period of use, regardless of whether any activity was recorded. This procedure is not required when the recording device and related software captures the user's unique identification and the date and time of each recording.

Members should document the existence of a recording in any report or other official record of the contact, including any instance where the recorder malfunctioned or the member deactivated the recording. Members should include the reason for deactivation.

424.6 ACTIVATION OF THE AUDIO/VIDEO RECORDER

This policy is not intended to describe every possible situation in which the recorder should be used, although there are many situations where its use is appropriate. Members should activate the recorder any time the member believes it would be appropriate or valuable to record an incident.

The recorder should be activated in any of the following situations:

(a) All enforcement and investigative contacts including stops and field interview situations

(b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops

(c) Self-initiated activity in which a deputy would normally notify the Dispatch Center

(d) Any other contact that becomes adversarial after the initial contact in a situation that would not otherwise require recording

Members should remain sensitive to the dignity of all individuals being recorded and exercise sound discretion to respect privacy by discontinuing recording whenever it reasonably appears to the member that such privacy may outweigh any legitimate law enforcement interest in recording. Requests by members of the public to stop recording should be considered using this same criterion. Recording should resume when privacy is no longer at issue unless the circumstances no longer fit the criteria for recording.

At no time is a member expected to jeopardize his/her safety in order to activate a portable recorder or change the recording media. However, the recorder should be activated in situations described above as soon as reasonably practicable.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

424.6.1 CESSATION OF RECORDING
Once activated, the portable recorder should remain on continuously until the member reasonably believes that his/her direct participation in the incident is complete or the situation no longer fits the criteria for activation. Recording may be stopped during significant periods of inactivity such as report writing or other breaks from direct participation in the incident.

424.6.2 SURREPTITIOUS USE OF THE AUDIO/VIDEO RECORDER
Virginia law permits an individual to surreptitiously record any conversation in which one party to the conversation has given his/her permission (Va. Code § 19.2-62).

Members may surreptitiously record any conversation during the course of a criminal investigation in which the member reasonably believes that such a recording will be lawful and beneficial to the investigation.

Members shall not surreptitiously record another department member without a court order unless lawfully authorized by the Sheriff or the authorized designee.

424.6.3 EXPLOSIVE DEVICE
Many portable recorders, including body-worn cameras and audio/video transmitters, emit radio waves that could trigger an explosive device. Therefore, these devices should not be used where an explosive device may be present.

424.7 PROHIBITED USE OF PORTABLE RECORDERS
Members are prohibited from using department-issued portable recorders and recording media for personal use and are prohibited from making personal copies of recordings created while on-duty or while acting in an official capacity Misuse of department-issued portable recorders and recording media may result in civil and criminal liability (Va. Code § 19.2-63.1).

Members are also prohibited from retaining recordings of activities or information obtained while on-duty, whether the recording was created with department-issued or personally owned recorders. Members shall not duplicate or distribute such recordings, except for authorized legitimate department business purposes. All such recordings shall be retained at the Department.

Members are prohibited from using personally owned recording devices while on-duty without the express consent of the Shift Supervisor. Any member who uses a personally owned recorder for department-related activities shall comply with the provisions of this policy, including retention and release requirements, and should notify the on-duty supervisor of such use as soon as reasonably practicable.

Recordings shall not be used by any member for the purpose of embarrassment, harassment or ridicule.

424.8 IDENTIFICATION AND PRESERVATION OF RECORDINGS
To assist with identifying and preserving data and recordings, members should download, tag or mark these in accordance with procedure and document the existence of the recording in any related case report.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

A member should transfer, tag or mark recordings when the member reasonably believes:

(a) The recording contains evidence relevant to potential criminal, civil or administrative matters.

(b) A complainant, victim or witness has requested non-disclosure.

(c) A complainant, victim or witness has not requested non-disclosure but the disclosure of the recording may endanger the person.

(d) Disclosure may be an unreasonable violation of someone’s privacy.

(e) Medical or mental health information is contained.

(f) Disclosure may compromise an undercover officer or confidential informant.

Any time a member reasonably believes a recorded contact may be beneficial in a non-criminal matter (e.g., a hostile contact), the member should promptly notify a supervisor of the existence of the recording.

424.9 RETENTION OF RECORDINGS

All recordings shall be retained for a period consistent with the requirements of the established records retention schedule but in no event for a period less than 180 days.

424.9.1 RELEASE OF AUDIO/VIDEO RECORDINGS

Requests for the release of audio/video recordings shall be processed in accordance with the Records Maintenance and Release Policy.

424.10 REVIEW OF RECORDED MEDIA FILES

When preparing written reports, members should review their recordings as a resource (See the Officer-Involved Shootings and Deaths Policy for guidance in those cases).

However, members shall not retain personal copies of recordings. Members should not use the fact that a recording was made as a reason to write a less detailed report.

Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct or whenever such recordings would be beneficial in reviewing a member's performance.

Recorded files may also be reviewed:

(a) Upon approval by a supervisor, by any member of the Department who is participating in an official investigation, such as a personnel complaint, administrative investigation or criminal investigation.

(b) Pursuant to lawful process or by court personnel who are otherwise authorized to review evidence in a related case.

(c) In compliance with a public records request, if permitted, and in accordance with the Records Maintenance and Release Policy.

All recordings should be reviewed by the Custodian of Records prior to public release (see the Records Maintenance and Release Policy).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Public Recording of Law Enforcement Activity

425.1 PURPOSE AND SCOPE

This policy provides guidelines for handling situations in which members of the public photograph or audio/video record law enforcement actions and other public activities that involve members of this department. In addition, this policy provides guidelines for situations where the recordings may be evidence.

425.2 POLICY

The Madison County Sheriff's Office recognizes the right of persons to lawfully record members of this department who are performing their official duties. Members of this department will not prohibit or intentionally interfere with such lawful recordings. Any recordings that are deemed to be evidence of a crime or relevant to an investigation will only be collected or seized lawfully.

Deputies should exercise restraint and should not resort to highly discretionary arrests for offenses such as interference, failure to comply or disorderly conduct as a means of preventing someone from exercising the right to record members performing their official duties.

425.3 RECORDING LAW ENFORCEMENT ACTIVITY

Members of the public who wish to record law enforcement activities are limited only in certain aspects.

(a) Recordings may be made from any public place or any private property where the individual has the legal right to be present.

(b) Beyond the act of photographing or recording, individuals may not interfere with the law enforcement activity. Examples of interference include, but are not limited to:

1. Tampering with a witness or suspect.
2. Inciting others to violate the law.
3. Being so close to the activity as to present a clear safety hazard to the deputies.
4. Being so close to the activity as to interfere with a deputy’s effective communication with a suspect or witness.

(c) The individual may not present an undue safety risk to the deputy, him/herself or others.

425.4 DEPUTY RESPONSE

Deputies should promptly request that a supervisor respond to the scene whenever it appears that anyone recording activities may be interfering with an investigation or it is believed that the recording may be evidence. If practicable, deputies should wait for the supervisor to arrive before taking enforcement action or seizing any cameras or recording media.

Whenever practicable, deputies or supervisors should give clear and concise warnings to individuals who are conducting themselves in a manner that would cause their recording or behavior to be unlawful. Accompanying the warnings should be clear directions on what an

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

individual can do to be compliant; directions should be specific enough to allow compliance. For example, rather than directing an individual to clear the area, a deputy could advise the person that he/she may continue observing and recording from the sidewalk across the street.

If an arrest or other significant enforcement activity is taken as the result of a recording that interferes with law enforcement activity, deputies shall document in a report the nature and extent of the interference or other unlawful behavior and the warnings that were issued.

425.5 SUPERVISOR RESPONSIBILITIES

A supervisor should respond to the scene when requested or any time the circumstances indicate a likelihood of interference or other unlawful behavior.

The supervisor should review the situation with the deputy and:

(a) Request any additional assistance as needed to ensure a safe environment.

(b) Take a lead role in communicating with individuals who are observing or recording regarding any appropriate limitations on their location or behavior. When practical, the encounter should be recorded.

(c) When practicable, allow adequate time for individuals to respond to requests for a change of location or behavior.

(d) Ensure that any enforcement, seizure or other actions are consistent with this policy and constitutional and state law.

(e) Explain alternatives for individuals who wish to express concern about the conduct of department members, such as how and where to file a complaint.

425.6 SEIZING RECORDINGS AS EVIDENCE

Deputies should not seize recording devices or media unless (42 USC § 2000aa):

(a) There is probable cause to believe the person recording has committed or is committing a crime to which the recording relates, and the recording is reasonably necessary for prosecution of the person.

1. Absent exigency or consent, a warrant should be sought before seizing or viewing such recordings. Reasonable steps may be taken to prevent erasure of the recording.

(b) There is reason to believe that the immediate seizure of such recordings is necessary to prevent serious bodily injury or death of any person.

(c) The person consents.

1. To ensure that the consent is voluntary, the request should not be made in a threatening or coercive manner.

2. If the original recording is provided, a copy of the recording should be provided to the recording party, if practicable. The recording party should be permitted to be present while the copy is being made, if feasible. Another way to obtain the evidence is to transmit a copy of the recording from a device to a department-owned device.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Public Recording of Law Enforcement Activity

Recording devices and media that are seized will be submitted within the guidelines of the Property and Evidence Section Policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Automated License Plate Readers (ALPRs)

426.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

426.2 POLICY

The policy of the Madison County Sheriff's Office is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

426.3 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Madison County Sheriff's Office to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Administration Division Supervisor. The Administration Division Supervisor will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

426.4 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

(a) An ALPR shall only be used for official law enforcement business.

(b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped vehicles to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

(d) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(e) No ALPR operator may access confidential department, state or federal data unless authorized to do so.

(f) If practicable, the deputy should verify an ALPR response through the appropriate official law enforcement database before taking enforcement action that is based solely on an ALPR alert.

426.5 DATA COLLECTION AND RETENTION

The Administration Division Supervisor is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

All stored ALPR data should be retained in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances, the applicable data should be downloaded onto portable media and booked into evidence.

426.6 ACCOUNTABILITY

All data will be closely safeguarded and protected by both procedural and technological means. The Madison County Sheriff's Office will observe the following safeguards regarding access to and use of stored data:

(a) All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(b) Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(c) ALPR system audits should be conducted on a regular basis.

426.7 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

(a) The agency makes a written request for the ALPR data that includes:

1. The name of the agency.
2. The name of the person requesting.
3. The intended purpose of obtaining the information.

(b) The request is reviewed by the Administration Division Supervisor or the authorized designee and approved before the request is fulfilled.

(c) The approved request is retained on file.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Automated License Plate Readers (ALPRs)

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Homeless Persons

427.1 PURPOSE AND SCOPE

The purpose of this policy is to ensure that department members understand the needs and rights of the homeless, and to establish procedures to guide them during all contacts with the homeless, whether consensual or for enforcement purposes.

This policy establishes a liaison to the homeless community, addresses the responsibilities of the department member appointed to act as a liaison to the homeless, and details the need for special protection and services for homeless persons.

427.2 POLICY

It is the policy of the Madison County Sheriff's Office to protect the rights, dignity and private property of all members of the community, including people who are homeless. Abuse of authority to harass any member of the community will not be permitted. The Madison County Sheriff's Office will address the needs of homeless persons in balance with the overall mission of this department.

Homelessness is not a crime and members will not use homelessness as the sole basis for detention or law enforcement action.

427.3 LIAISON TO THE HOMELESS COMMUNITY

The Sheriff shall delegate certain responsibilities to a liaison to the homeless community. The liaison shall be appointed by and directly responsible to the Patrol Division Supervisor or the authorized designee.

The responsibilities of the liaison include, but are not limited to:

(a) Maintaining and making available to all department members a list of assistance programs and other resources that are available to homeless persons.

(b) Meeting with social services and representatives of other organizations that render assistance to the homeless community.

(c) Maintaining a list of the areas within and near the jurisdiction of this department that are used as frequent homeless encampments.

(d) Remaining abreast of laws dealing with homelessness, including personal property rights.

(e) Being present during any clean-up operation conducted by this department that involves the removal of personal property of the homeless. This is to ensure that the established rights of the homeless are not violated.

(f) Developing training to assist members in understanding current legal and social issues relating to the homeless.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

427.4 FIELD CONTACTS

Deputies are encouraged to contact a homeless person to render aid, offer assistance or to check on the person's welfare. Deputies also will take enforcement action when information supports a reasonable and articulable suspicion of criminal activity. However, such contacts shall not be used for harassment.

When encountering a homeless person who has committed a nonviolent misdemeanor and continued freedom is not likely to result in a continuation of the offense or a breach of the peace, deputies are encouraged to consider long-term solutions, such as shelter referrals and counseling, in lieu of an arrest and criminal charges.

Deputies should provide homeless persons with resources and assistance information whenever it is reasonably apparent that such services may be appropriate.

427.4.1 CONSIDERATIONS

A homeless person will receive the same level and quality of service provided to other members of the community. The fact that a victim, witness or suspect is homeless can, however, require special consideration for a successful investigation and prosecution. When handling investigations involving victims, witnesses or suspects who are homeless, deputies should consider:

(a) Documenting alternate contact information. This may include obtaining addresses and telephone numbers of relatives and friends.

(b) Documenting locations the person may frequent.

(c) Providing victim/witness resources, when appropriate.

(d) Obtaining sufficient statements from all available witnesses in the event that a victim cannot be located and is unavailable for a court appearance.

(e) Arranging for transportation for investigation-related matters, such as medical exams and court appearances.

(f) Whether a crime should be reported and submitted for prosecution, even when a victim who is homeless indicates that he/she does not desire prosecution.

(g) Whether the person may be an adult abuse victim and, if so, proceed in accordance with the Adult Abuse Policy.

427.5 MENTAL HEALTH ISSUES

When mental health issues are evident, deputies should consider referring the person to the appropriate mental health agency or providing the person with contact information for mental health assistance, as appropriate. In these circumstances, deputies may provide transportation to a mental health facility for voluntary evaluation if it is requested or offered and accepted by the person, and approved by a supervisor. Deputies should consider detaining the person under civil commitment when facts and circumstances reasonably indicate such a detention is warranted (see the Civil Commitments Policy).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

427.6 PERSONAL PROPERTY

The personal property of homeless persons must not be treated differently than the property of other members of the community. Deputies should use reasonable care when handling, collecting and retaining the personal property of homeless persons and should not destroy or discard the personal property of a homeless person.

When a homeless person is arrested or otherwise removed from a public place, deputies should make reasonable accommodations to permit the person to lawfully secure his/her personal property. Otherwise, it should be collected for safekeeping. If the arrestee has more personal property than can reasonably be collected and transported by the deputy, a supervisor should be consulted. The property should be photographed and measures should be taken to remove or secure it. It will be the supervisor’s responsibility to coordinate its removal and safekeeping.

Deputies should not conduct or assist in clean-up operations of belongings that reasonably appear to be the property of homeless persons without the prior authorization of a supervisor or the homeless liaison. When practicable, requests by the public for clean-up of a homeless encampment should be referred to the liaison.

Deputies who encounter unattended encampments, bedding or other personal property in public areas that reasonably appears to belong to a homeless person should not remove or destroy such property and should inform the liaison if such property appears to involve a trespass, is a blight to the community or is the subject of a complaint. It will be the responsibility of the liaison to address the matter in a timely fashion.

427.7 ECOLOGICAL ISSUES

Sometimes homeless encampments can have an impact on the ecology and natural resources of the community and may involve criminal offenses beyond mere littering. Deputies are encouraged to notify other appropriate agencies or County departments when a significant impact to the environment has or is likely to occur. A significant impact to the environment may warrant a crime report, investigation, supporting photographs and supervisor notification.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Medical Marijuana

428.1 PURPOSE AND SCOPE

The purpose of this policy is to provide members of this department with guidelines for investigating the acquisition, possession, transportation, delivery, production, or use of marijuana under Virginia's medical marijuana laws (Va. Code § 54.1-3400 et seq.).

428.1.1 DEFINITIONS

Definitions related to this policy include (Va. Code § 54.1-3408.3; 18 VAC 110-60-10):

Cannabis product - A product that is produced by a pharmaceutical processor, registered with the Board of Pharmacy, and that is composed of cannabis oil, botanical cannabis, or other substances as allowed by Virginia law.

Registered agent - A designated individual registered with the Board of Pharmacy with authority to receive a cannabis product for a patient.

Written certification - A certification issued by a qualifying medical practitioner to a qualifying patient for the use of a cannabis product.

428.2 POLICY

It is the policy of the Madison County Sheriff's Office to prioritize resources to avoid making arrests related to marijuana that the arresting deputy reasonably believes would not be prosecuted by state or federal authorities.

Virginia medical marijuana laws are intended to provide protection from prosecution to those who use, possess, deliver, or produce marijuana for treatment or to alleviate the symptoms of a patient's diagnosed medical condition or disease. However, Virginia medical marijuana laws do not affect federal laws, and there is no medical exception under federal law for the possession or distribution of marijuana. The Madison County Sheriff's Office will exercise discretion to ensure laws are appropriately enforced without unreasonably burdening both those individuals protected under Virginia law and the resources of the Department.

428.3 INVESTIGATION

Investigations involving the possession, delivery, production, or use of marijuana generally fall into two categories:

(a) Investigations when a medicinal claim is made.

(b) Investigations when no person makes a medicinal claim.

428.3.1 INVESTIGATIONS INVOLVING A MEDICAL CLAIM

Deputies should not take enforcement action against a lawfully registered patient or registered agent who is able to provide sufficient proof of lawful registration for obtaining, possessing, transporting, or using medical marijuana (Va. Code § 54.1-3408.3; 18 VAC 110-60-50).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Deputies should investigate a claim made by a person that the person is lawfully qualified to possess marijuana for medical purposes when that person does not provide sufficient proof of lawful registration and should not take enforcement action against the person if the claim appears to be valid.

Employees of nursing homes, hospice, hospice facilities, and assisted living facilities who are authorized to possess, distribute, or administer medications to patients or residents are permitted to store, dispense, and administer medical marijuana to patients or residents issued written certifications and registered with the Board of Pharmacy (Va. Code § 18.2-251.1:2; Va. Code § 32.1-127; Va. Code § 32.1-162.6:1; Va. Code § 63.2-1803.01).

428.3.2 INVESTIGATIONS WITH NO MEDICAL CLAIM

In any investigation involving the possession, delivery, production, or use of marijuana or drug paraphernalia where no person claims that the marijuana is used for medicinal purposes, the deputy should proceed with a criminal investigation. Deputies should consider that certain amounts may be permitted for personal use (Va. Code § 4.1-1100 et seq.). A medicinal defense may be raised at any time, so deputies should document any statements and observations that may be relevant to whether the marijuana was possessed or produced for medicinal purposes.

428.4 FEDERAL LAW ENFORCEMENT

Deputies should provide information regarding a marijuana investigation to federal law enforcement authorities when it is requested by federal law enforcement authorities or whenever the deputy believes those authorities would have a particular interest in the information.

428.5 EVIDENCE

428.5.1 MEMBER RESPONSIBILITIES

The investigating member should notify the receiving Property and Evidence Section member in writing when marijuana may be the subject of a medical claim.

428.5.2 PROPERTYBUREAU SUPERVISOR RESPONSIBILITIES

The Property and Evidence Section supervisor should ensure that marijuana, drug paraphernalia, or other related property seized from a person engaged or assisting in the use of medical marijuana is not destroyed. The Property and Evidence Section supervisor is not responsible for caring for live marijuana plants.

Upon the prosecutor’s decision to forgo prosecution, or the dismissal of charges or an acquittal, the Property and Evidence Section supervisor should, as soon as practicable, return to the person from whom it was seized any useable marijuana, drug paraphernalia, or other related property.

The Property and Evidence Section supervisor may release marijuana to federal law enforcement authorities upon presentation of a valid court order or by a written order of the Investigation Division supervisor.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Medical Aid and Response

429.1 PURPOSE AND SCOPE

This policy recognizes that members often encounter persons in need of medical aid and establishes a law enforcement response to such situations.

429.2 POLICY

It is the policy of the Madison County Sheriff's Office that all deputies and other designated members be trained to provide emergency medical aid and to facilitate an emergency medical response.

429.3 FIRST RESPONDING MEMBER RESPONSIBILITIES

Whenever practicable, members should take appropriate steps to provide initial medical aid (e.g., first aid, CPR, use of an automated external defibrillator (AED)) in accordance with their training and current certification levels. This should be done for those in need of immediate care and only when the member can safely do so.

Prior to initiating medical aid, the member should contact the Dispatch Center and request response by Emergency Medical Services (EMS) as the member deems appropriate.

Members should follow universal precautions when providing medical aid, such as wearing gloves and avoiding contact with bodily fluids, consistent with the Communicable Diseases Policy. Members should use a barrier or bag device to perform rescue breathing.

When requesting EMS, the member should provide the Dispatch Center with information for relay to EMS personnel in order to enable an appropriate response, including:

(a) The location where EMS is needed.

(b) The nature of the incident.

(c) Any known scene hazards.

(d) Information on the person in need of EMS, such as:

1. Signs and symptoms as observed by the member.
2. Changes in apparent condition.
3. Number of patients, sex, and age, if known.
4. Whether the person is conscious, breathing, and alert, or is believed to have consumed drugs or alcohol.
5. Whether the person is showing signs of extreme agitation or is engaging in violent irrational behavior accompanied by profuse sweating, extraordinary strength beyond their physical characteristics, and imperviousness to pain.

Members should stabilize the scene whenever practicable while awaiting the arrival of EMS.

Members should not direct EMS personnel regarding whether to transport the person for treatment.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

429.4 TRANSPORTING ILL AND INJURED PERSONS

Except in exceptional cases where alternatives are not reasonably available, members should not transport persons who are unconscious, who have serious injuries, or who may be seriously ill. EMS personnel should be called to handle patient transportation.

Deputies should search any person who is in custody before releasing that person to EMS for transport.

A deputy should accompany any person in custody during transport in an ambulance when requested by EMS personnel, when it reasonably appears necessary to provide security, when it is necessary for investigative purposes, or when so directed by a supervisor.

Members should not provide emergency escort for medical transport or civilian vehicles.

429.5 PERSONS REFUSING EMS CARE

If a person who is not in custody refuses EMS care or refuses to be transported to a medical facility, a deputy shall not force that person to receive medical care or be transported.

However, members may assist EMS personnel when EMS personnel determine the person lacks the mental capacity to understand the consequences of refusing medical care or to make an informed decision and the lack of immediate medical attention may result in serious bodily injury or the death of the person.

In cases where mental illness may be a factor, the deputy should consider proceeding with a civil commitment or an involuntary commitment in accordance with the Civil Commitments Policy.

If a deputy believes that a person who is in custody requires EMS care and the person refuses, he/she should encourage the person to receive medical treatment. The deputy may also consider contacting a family member to help persuade the person to agree to treatment or who may be able to authorize treatment for the person.

If the person who is in custody still refuses, the deputy will require the person to be transported to the nearest medical facility. In such cases, the deputy should consult with a supervisor prior to the transport.

Members shall not sign refusal-for-treatment forms or forms accepting financial responsibility for treatment.

429.6 SICK OR INJURED ARRESTEE

If an arrestee appears ill or injured, or claims illness or injury, he/she should be medically cleared prior to booking. If the deputy has reason to believe the arrestee is feigning injury or illness, the deputy should contact a supervisor, who will determine whether medical clearance will be obtained prior to booking.

If the jail or detention facility refuses to accept custody of an arrestee based on medical screening, the deputy should note the name of the facility person refusing to accept custody and the reason for refusal, and should notify a supervisor to determine the appropriate action.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Arrestees who appear to have a serious medical issue should be transported by ambulance. Deputies shall not transport an arrestee to a hospital without a supervisor’s approval.

Nothing in this section should delay a deputy from requesting EMS when an arrestee reasonably appears to be exhibiting symptoms that appear to be life threatening, including breathing problems or an altered level of consciousness, or is claiming an illness or injury that reasonably warrants an EMS response in accordance with the deputy’s training.

429.7 MEDICAL ATTENTION RELATED TO USE OF FORCE

Specific guidelines for medical attention for injuries sustained from a use of force may be found in the Use of Force, Handcuffing and Restraints, Control Devices and Conducted Energy Device policies.

429.8 AIR AMBULANCE

Generally, when on-scene, EMS personnel will be responsible for determining whether an air ambulance response should be requested. An air ambulance may be appropriate when there are victims with life-threatening injuries or who require specialized treatment (e.g., gunshot wounds, burns, obstetrical cases), and distance or other known delays will affect the EMS response.

The Madison County Fire Department should develop guidelines for air ambulance landings or enter into local operating agreements for the use of air ambulances, as applicable. In creating those guidelines, the Department should identify:

- Responsibility and authority for designating a landing zone and determining the size of the landing zone.
- Responsibility for securing the area and maintaining that security once the landing zone is identified.
- Consideration of the air ambulance provider's minimum standards for proximity to vertical obstructions and surface composition (e.g., dirt, gravel, pavement, concrete, grass).
- Consideration of the air ambulance provider's minimum standards for horizontal clearance from structures, fences, power poles, antennas, or roadways.
- Responsibility for notifying the appropriate highway or transportation agencies if a roadway is selected as a landing zone.
- Procedures for ground personnel to communicate with flight personnel during the operation.

One member of the Madison County Fire Department at the scene should be designated as the air ambulance communications contact. Headlights, spotlights, and flashlights should not be aimed upward at the air ambulance. Members should direct vehicle and pedestrian traffic away from the landing zone and provide assistance to the Fire Department as requested.

Members shall follow these cautions when near an air ambulance:

- Never approach the aircraft until signaled by the flight crew.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

- Always approach the aircraft from the front.
- Avoid the aircraft's tail rotor area.
- Wear eye protection during the landing and take-off.
- Do not carry or hold items, such as IV bags, above the head.
- Ensure that no one smokes near the aircraft.

429.9 AUTOMATED EXTERNAL DEFIBRILLATOR (AED) USE

429.9.1 AED USER RESPONSIBILITY

Members who are issued AEDs for use in department vehicles should check the AED at the beginning of the shift to ensure it is properly charged and functioning. Any AED that is not functioning properly will be taken out of service and given to the Training Supervisor who is responsible for ensuring that all defective AEDs are turned over to the Madison County Emergency Medical Services (EMS) for repairs.

Following use of an AED, the device shall be cleaned and/or decontaminated as required. The electrodes and/or pads will be replaced as recommended by the AED manufacturer as required.

Any member who uses an AED should contact the Dispatch Center as soon as possible and request response by EMS.

429.9.2 AED REPORTING

Any member using an AED will complete an incident report detailing its use.

429.9.3 AED TRAINING AND MAINTENANCE

The Training Supervisor should ensure appropriate training is provided to members authorized to use an AED.

The Madison County Emergency Services is responsible for ensuring AED devices are appropriately maintained and will retain records of all maintenance in accordance with the established records retention schedule.

429.10 ADMINISTRATION OF OPIOID OVERDOSE MEDICATION

Trained members may administer opioid overdose medication to a person experiencing an opiate-related overdose in accordance with protocols developed by the Board of Pharmacy (Va. Code § 54.1-3408(X)).

429.10.1 OPIOID OVERDOSE MEDICATION USER RESPONSIBILITIES

Members who are qualified to administer opioid overdose medication, such as naloxone, should handle, store, and administer the medication consistent with their training. Members should check the medication and associated administration equipment at the beginning of their shift to ensure they are serviceable and not expired. Any expired medication or unserviceable administration equipment should be removed from service and given to the Training Supervisor.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

See attachment: 410 Statewide Standing Order for Naloxone (1-14-2022).pdf

Any member who administers an opioid overdose medication should contact the Dispatch Center as soon as possible and request response by EMS.

429.10.2 OPIOID OVERDOSE MEDICATION REPORTING
Any member administering opioid overdose medication should detail its use in an appropriate report.

See attachment: Naloxone Reporting Form.pdf

429.10.3 OPIOID OVERDOSE MEDICATION TRAINING
The Training Supervisor should ensure training is provided to members authorized to administer opioid overdose medication.

429.11 ADMINISTRATION OF EPINEPHRINE IN THE MADISON COUNTY SHERIFF'S DEPARTMENT FACILITY

Trained members may administer epinephrine to a person believed in good faith to be having an anaphylactic reaction in those areas of the Madison County Sheriff's Office facility used by the general public (Va. Code § 15.2-2820; Va. Code § 54.1-3408; Va. Code § 54.1-3408.5).

429.11.1 EPINEPHRINE USER RESPONSIBILITIES
Members who are qualified to administer epinephrine should handle, store, and administer the medication consistent with their training. Members should check the medication and associated administration equipment at the beginning of their shift to ensure they are serviceable and not expired. Any expired medication or unserviceable administration equipment should be removed from service and given to the Training Supervisor.

While the Madison County Sheriff's Department does not issue emergency epinephrine, members who are properly trained in its administration may administer epinephrine if it is available and medically indicated. Any member who administers epinephrine should contact the Dispatch Center as soon as possible and request response by EMS.

429.11.2 EPINEPHRINE REPORTING
Any member administering epinephrine should detail its use in an appropriate report.

429.11.3 EPINEPHRINE TRAINING
The Training Supervisor should ensure training is provided to members authorized to administer epinephrine (Va. Code § 54.1-3408; Va. Code § 54.1-3408.5).

429.12 FIRST AID TRAINING

Subject to available resources, the Training Supervisor should ensure deputies receive periodic first aid training appropriate for their position.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

First Amendment Assemblies

430.1 PURPOSE AND SCOPE

This policy provides guidance for responding to public assemblies or demonstrations.

430.2 POLICY

The Madison County Sheriff's Office respects the rights of people to peaceably assemble. It is the policy of this department not to unreasonably interfere with, harass, intimidate or discriminate against persons engaged in the lawful exercise of their rights, while also preserving the peace, protecting life and preventing the destruction of property.

430.3 GENERAL CONSIDERATIONS

Individuals or groups present on the public way, such as public facilities, streets or walkways, generally have the right to assemble, rally, demonstrate, protest or otherwise express their views and opinions through varying forms of communication, including the distribution of printed matter (Va. Const. art. I, § 12).

These rights may be limited by laws or ordinances regulating such matters as:

- Committing acts of terrorism (Va. Code § 18.2-46.5)
- Participating in paramilitary activity (Va. Code § 18.2-433.2)
- Rioting (Va. Code § 18.2-405)
- Committing acts of violence by a mob (Va. Code § 18.2-42.1)
- Partaking in unlawful assembly (Va. Code § 18.2-406)
- Displaying disorderly conduct (Va. Code § 18.2-415)
- Burning objects (Va. Code § 18.2-423.01)
- Wearing masks (Va. Code § 18.2-422)
- Unlawful picketing (Va. Code § 40.1-53)
- Crossing law enforcement lines (Va. Code § 18.2-414.2)
- Trespassing (Va. Code § 18.2-119)
- Obstructing free passage of others (Va. Code § 18.2-404)
- Resisting or obstructing execution of legal process (Va. Code § 18.2-409)

However, deputies shall not take action or fail to take action based on the opinions being expressed.

Participant behavior during a demonstration or other public assembly can vary. This may include, but is not limited to:

- Lawful, constitutionally protected actions and speech.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

- Civil disobedience (typically involving minor criminal acts).
- Rioting.

All of these behaviors may be present during the same event. Therefore, it is imperative that law enforcement actions are measured and appropriate for the behaviors deputies may encounter. This is particularly critical if force is being used. Adaptable strategies and tactics are essential.

The purpose of a law enforcement presence at the scene of public assemblies and demonstrations should be to preserve the peace, to protect life and to prevent the destruction of property.

Deputies should not:

(a) Engage in assembly or demonstration-related discussion with participants.

(b) Harass, confront or intimidate participants.

(c) Seize the cameras, cell phones or materials of participants or observers unless a deputy is placing a person under lawful arrest.

Supervisors should continually observe department members under their commands to ensure that members' interaction with participants and their response to crowd dynamics is appropriate.

430.3.1 PHOTOGRAPHS, VIDEO RECORDINGS AND OTHER INFORMATION

Photographs, video recordings and other information may be collected at assemblies and demonstrations as they can serve a number of purposes, such as support of criminal prosecutions, assistance in evaluating department performance, serving as training material, recording the use of dispersal orders and facilitating a response to allegations of improper law enforcement conduct.

Photographs, video recordings and other information shall not be maintained on the political, religious or social activities, views or associations of any individual, group or organization unless those activities, views or associations directly relate to an investigation of criminal activity and there is reasonable suspicion that the subject of the information is involved in criminal conduct.

430.4 UNPLANNED EVENTS

When responding to an unplanned or spontaneous public gathering, the first responding deputy should conduct an assessment of conditions, including, but not limited to:

- Location.
- Number of participants.
- Apparent purpose of the event.
- Leadership (whether it is apparent and/or whether it is effective).
- Any initial indicators of unlawful or disruptive activity.
- Indicators that lawful use of public facilities, streets or walkways will be impacted.
- Ability and/or need to continue monitoring the incident.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Initial assessment information should be promptly communicated to the Dispatch Center, and the assignment of a supervisor should be requested. Additional resources should be requested as appropriate. The responding supervisor shall assume command of the incident until command is expressly assumed by another, and the assumption of command is communicated to the involved members. A clearly defined command structure that is consistent with the Incident Command System (ICS) should be established as resources are deployed.

430.5 PLANNED EVENT PREPARATION

For planned events, comprehensive, incident-specific operational plans should be developed. The ICS should be considered for such events.

430.5.1 INFORMATION GATHERING AND ASSESSMENT

In order to properly assess the potential impact of a public assembly or demonstration on public safety and order, relevant information should be collected and vetted. This may include:

- Information obtained from outreach to group organizers or leaders.
- Information about past and potential unlawful conduct associated with the event or similar events.
- The potential time, duration, scope, and type of planned activities.
- Any other information related to the goal of providing a balanced response to criminal activity and the protection of public safety interests.

Information should be obtained in a transparent manner, and the sources documented. Relevant information should be communicated to the appropriate parties in a timely manner.

Information will be obtained in a lawful manner and will not be based solely on the purpose or content of the assembly or demonstration, or actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability of the participants (or any other characteristic that is unrelated to criminal conduct or the identification of a criminal subject).

430.5.2 OPERATIONAL PLANS

An operational planning team with responsibility for event planning and management should be established. The planning team should develop an operational plan for the event.

The operational plan will minimally provide for:

(a) Command assignments, chain of command structure, roles and responsibilities.

(b) Staffing and resource allocation.

(c) Management of criminal investigations.

(d) Designation of uniform of the day and related safety equipment (helmets, shields, etc.).

(e) Deployment of specialized resources.

(f) Event communications and interoperability in a multijurisdictional event.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(g) An established liaison with demonstration leaders and external agencies.

(h) An established liaison with County government and legal staff.

(i) Media relations.

(j) Logistics: food, fuel, replacement equipment, duty hours, relief and transportation.

(k) Traffic management plans.

(l) First aid and emergency medical service provider availability.

(m) Prisoner transport and detention.

(n) Review of policies regarding public assemblies and use of force in crowd control.

(o) Parameters for declaring an unlawful assembly.

(p) Arrest protocol, including management of mass arrests.

(q) Protocol for recording information flow and decisions.

(r) Rules of engagement, including rules of conduct, protocols for field force extraction and arrests, and any authorization required for the use of force.

(s) Protocol for handling complaints during the event.

(t) Parameters for the use of body-worn cameras and other portable recording devices.

430.5.3 MUTUAL AID AND EXTERNAL RESOURCES

The magnitude and anticipated duration of an event may necessitate interagency cooperation and coordination. The assigned Incident Commander should ensure that any required memorandums of understanding or other agreements are properly executed, and that any anticipated mutual aid is requested and facilitated (see the Outside Agency Assistance Policy).

430.6 UNLAWFUL ASSEMBLY DISPERSAL ORDERS

If a public gathering or demonstration remains peaceful and nonviolent, and there is no reasonably imminent threat to persons or property, the Incident Commander should generally authorize continued monitoring of the event.

Should the Incident Commander make a determination that public safety is presently or is about to be jeopardized, he/she or the authorized designee should attempt to verbally persuade event organizers or participants to disperse of their own accord. Warnings and advisements may be communicated through established communications links with leaders and/or participants or to the group (Va. Code § 18.2-411).

When initial attempts at verbal persuasion are unsuccessful, the Incident Commander or the authorized designee should make a clear, standardized announcement to the gathering that the event is an unlawful assembly, and should order the dispersal of the participants. The announcement should be communicated by whatever methods are reasonably available to ensure that the content of the message is clear and that it has been heard by the participants. The

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

announcement should be amplified, made in different languages as appropriate, made from multiple locations in the affected area and documented by audio and video. The announcement should provide information about what law enforcement actions will take place if illegal behavior continues and should identify routes for egress. A reasonable time to disperse should be allowed following a dispersal order.

430.7 USE OF FORCE

Use of force is governed by current department policy and applicable law (see the Use of Force, Handcuffing and Restraints, Control Devices, and Conducted Energy Device policies).

Individuals refusing to comply with lawful orders (e.g., nonviolent refusal to disperse) should be given a clear verbal warning and a reasonable opportunity to comply. If an individual refuses to comply with lawful orders, the Incident Commander shall evaluate the type of resistance and adopt a reasonable response in order to accomplish the law enforcement mission (such as dispersal or arrest of those acting in violation of the law). Control devices and conducted energy devices should be considered only when the participants' conduct reasonably appears to present the potential to harm deputies, themselves or others, or will result in substantial property loss or damage (see the Control Devices and the Conducted Energy Device policies).

Force or control devices, including oleoresin capsaicin (OC), should be directed toward individuals and not toward groups or crowds, unless specific individuals cannot reasonably be targeted due to extreme circumstances, such as a riotous crowd.

Any use of force by a member of this department shall be documented promptly, completely, and accurately in an appropriate report. The type of report required may depend on the nature of the incident.

430.8 ARRESTS

The Madison County Sheriff's Office should respond to unlawful behavior in a manner that is consistent with the operational plan. If practicable, warnings or advisements should be communicated prior to arrest.

Mass arrests should be employed only when alternate tactics and strategies have been or reasonably appear likely to be unsuccessful. Mass arrests shall only be undertaken upon the order of the Incident Commander or the authorized designee. There must be probable cause for each arrest.

If employed, mass arrest protocols should fully integrate:

(a) Reasonable measures to address the safety of deputies and arrestees.

(b) Dedicated arrest, booking and report writing teams.

(c) Timely access to medical care.

(d) Timely access to legal resources.

(e) Timely processing of arrestees.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(f) Full accountability for arrestees and evidence.

(g) Coordination and cooperation with the prosecuting authority, jail and courts (see the Citation Releases Policy).

430.9 MEDIA RELATIONS

The Public Information Officer should use all available avenues of communication, including press releases, briefings, press conferences and social media, to maintain open channels of communication with media representatives and the public about the status and progress of the event, taking all opportunities to reassure the public about the professional management of the event (see the Media Relations Policy).

430.10 DEMOBILIZATION

When appropriate, the Incident Commander or the authorized designee should implement a phased and orderly withdrawal of law enforcement resources. All relieved personnel should promptly complete any required reports, including use of force reports, and account for all issued equipment and vehicles to their supervisors prior to returning to normal operational duties.

430.11 POST EVENT

The Incident Commander should designate a member to assemble full documentation of the event, to include:

(a) Operational plan.

(b) Any incident logs.

(c) Any assignment logs.

(d) Vehicle, fuel, equipment and supply records.

(e) Incident, arrest, use of force, injury and property damage reports.

(f) Photographs, audio/video recordings, the Dispatch Center records/tapes.

(g) Media accounts (print and broadcast media).

430.11.1 AFTER-ACTION REPORTING

The Incident Commander should work with the County Attorney, as appropriate, to prepare a comprehensive after-action report of the event, explaining all incidents where force was used, to include:

(a) Date, time and description of the event.

(b) Actions taken and outcomes (e.g., injuries, property damage, arrests, costs).

(c) Problems identified.

(d) Significant events.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(e) Recommendations for improvement; opportunities for training should be documented in a generic manner, without identifying individuals or specific incidents, facts or circumstances.

430.12 TRAINING

Department members should receive periodic training regarding this policy, as well as the dynamics of crowd control and incident management. The Department should, when practicable, train with its external and mutual aid partners.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Civil Disputes

431.1 PURPOSE AND SCOPE

This policy provides members of the Madison County Sheriff's Office with guidance for addressing conflicts between persons when no criminal investigation or enforcement action is warranted (e.g., civil matters), with the goal of minimizing any potential for violence or criminal acts.

The Domestic or Family Violence Policy will address specific legal mandates related to domestic violence court orders. References in this policy to "court orders" apply to any order of a court that does not require arrest or enforcement by the terms of the order or by Virginia law.

431.2 POLICY

The Madison County Sheriff's Office recognizes that a law enforcement presence at a civil dispute can play an important role in the peace and safety of the community. Subject to available resources, members of this department will assist at the scene of civil disputes with the primary goal of safeguarding persons and property, preventing criminal activity and maintaining the peace. When handling civil disputes, members will remain impartial, maintain a calm presence, give consideration to all sides and refrain from giving legal or inappropriate advice.

431.3 GENERAL CONSIDERATIONS

When appropriate, members handling a civil dispute should encourage the involved parties to seek the assistance of resolution services or take the matter to the civil courts. Members must not become personally involved in disputes and shall at all times remain impartial.

While the following is not intended to be an exhaustive list, members should give consideration to the following when handling civil disputes:

(a) Civil disputes tend to be confrontational and members should be alert that they can escalate to violence very quickly. De-escalation techniques should be used when appropriate.

(b) Members should not dismiss alleged or observed criminal violations as a civil matter and should initiate the appropriate investigation and report when criminal activity is apparent.

(c) Members shall not provide legal advice; however, when appropriate, members should inform the parties when they are at risk of violating criminal laws.

(d) Members are reminded that they shall not enter a residence or other non-public location without legal authority.

(e) Members should not take an unreasonable amount of time assisting in these matters and generally should contact a supervisor if it appears that peacekeeping efforts longer than 30 minutes are warranted.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

431.4 COURT ORDERS

Disputes involving court orders can be complex. Where no mandate exists for a deputy to make an arrest for a violation of a court order, the matter should be addressed by documenting any apparent court order violation in a report. If there appears to be a more immediate need for enforcement action, the investigating deputy should consult a supervisor prior to making any arrest.

If a person appears to be violating the terms of a court order but is disputing the validity of the order or its applicability, the investigating deputy should document:

(a) The person's knowledge of the court order or whether proof of service exists.

(b) Any specific reason or rationale the involved person offers for not complying with the terms of the order.

A copy of the court order should be attached to the report when available. The report should be forwarded to the appropriate prosecutor. The report should also be forwarded to the court issuing the order with a notice that the report was also forwarded to the prosecutor for review.

431.4.1 STANDBY REQUESTS

The Madison County Sheriff's Office does not honor standby requests to assist citizens to obtain personal property from private premises in the absence of a court order. Participants in property disputes should consult their attorneys for advice as to how best to handle the recovery of personal property from private premises, or consult the courts as to how best to peaceably recover such property.

431.5 VEHICLES AND PERSONAL PROPERTY

Deputies may be faced with disputes regarding possession or ownership of vehicles or other personal property. Deputies may review documents provided by parties or available databases (e.g., vehicle registration), but should be aware that legal possession of vehicles or personal property can be complex. Generally, deputies should not take any enforcement action unless a crime is apparent. The people and the vehicle or personal property involved should be identified and the incident documented.

431.5.1 REPOSSESSIONS

Disputes over possession of personal or real property (e.g., land, homes, apartments) should generally be handled through a person seeking a court order. When a judge or magistrate issues an order or writ directing the Sheriff to seize and deliver property to the plaintiff a deputy acting pursuant to an order or writ shall (Va. Code § 8.01-114; Va. Code § 8.01-541):

(a) Upon receipt of the order or writ, endorse the date and time of receipt (Va. Code § 8.01-487).

(b) Serve a copy of the order or writ, including any attachments, on the judgment debtor or other responsible person at the premises where the levy is made (Va. Code § 8.01-487.1).

(c) Post the order or writ, including any attachments, on the front door of the premises if no one is present (Va. Code § 8.01-487.1).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Upon levying the order or writ, endorse the date and time of the levy (Va. Code § 8.01-487).

(e) Within 30 days of the date of the order or writ, file proof of service with the clerk of court.

(f) Prepare a report containing the following:

1. Date order or writ was received
2. Office tracking method
3. Nature of writ or order
4. Source of writ or order
5. Name of plaintiff/complainant and defendant/respondent
6. Name of the deputy assigned for service or serving deputy
7. Date of assignment
8. Method of service
9. Date of service
10. Location of service or attempted service
11. Reason for non-service

A deputy may, when necessary after refusal of admittance by the occupant, force entry to a dwelling during the daytime to execute an order or writ (Va. Code § 8.01-491).

431.6 REAL PROPERTY

Disputes over possession or occupancy of real property (e.g., land, homes, apartments) should generally be handled through a person seeking a court order.

431.6.1 WRITS OF EVICTION

A deputy executing a writ of eviction in an unlawful detainer case should confirm and document that notice of the date and time of eviction was served following expiration of the person's 10-day appeal period as required in Va. Code § 8.01-129.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Suspicious Activity Reporting

432.1 PURPOSE AND SCOPE

This policy provides guidelines for reporting and investigating suspicious and criminal activity.

432.1.1 DEFINITIONS

Definitions related to this policy include:

Involved party - An individual who has been observed engaging in suspicious activity, as defined in this policy, when no definitive criminal activity can be identified, thus precluding the person's identification as a suspect.

Suspicious activity - Any reported or observed activity that a member reasonably believes may have a nexus to any criminal act or attempted criminal act, or to foreign or domestic terrorism. Actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability should not be considered as factors that create suspicion (although these factors may be used as specific suspect descriptions). Examples of suspicious activity may include but are not limited to:

- Suspected pre-operational surveillance or intelligence gathering (e.g., photographing security features, asking questions about sensitive security-related subjects).
- Tests of security measures and response to incidents (e.g., "dry run," creating false alarms, attempts to enter secure areas without authorization).
- Suspicious purchases (e.g., purchasing large quantities of otherwise legal items, such as fertilizer, that could be used to create an explosive or other dangerous device).
- An individual in possession of such things as a hoax explosive or dispersal device, sensitive materials (e.g., passwords, access codes, classified government information), or coded or ciphered literature or correspondence.

Suspicious Activity Report (SAR) - An incident report used to document suspicious activity.

432.2 POLICY

The Madison County Sheriff's Office recognizes the need to protect the public from criminal conduct and acts of terrorism and shall lawfully collect, maintain and disseminate information regarding suspicious activities, while safeguarding civil liberties and privacy protections.

432.3 RESPONSIBILITIES

The Investigation Division Supervisor and the authorized designees will manage SAR activities. Authorized designees should include supervisors who are responsible for department participation in criminal intelligence systems as outlined in the Criminal Organizations Policy.

The responsibilities of the Investigation Division include, but are not limited to:

(a) Remaining familiar with those databases available to the department that would facilitate the purpose of this policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Maintaining adequate training in the area of intelligence gathering to ensure no information is being maintained that would violate the law or civil rights of any individual.

(c) Ensuring a process is available that would allow members to report relevant information. The process should be designed to promote efficient and quick reporting, and should not be cumbersome, duplicative or complicated.

(d) Ensuring that members are made aware of the purpose and value of documenting information regarding suspicious activity, as well as the databases and other information resources that are available to the Department.

(e) Ensuring that SAR information is appropriately disseminated to members in accordance with their job responsibilities.

(f) Coordinating investigative follow-up, if appropriate.

(g) Coordinating with any appropriate agency or fusion center.

(h) Ensuring that, as resources are available, the Department conducts outreach that is designed to encourage community members to report suspicious activity and that outlines what they should look for and how they should report it (e.g., website, public service announcements).

432.4 REPORTING AND INVESTIGATION

Any department member receiving information regarding suspicious activity should take any necessary immediate and appropriate action, including a request for tactical response or immediate notification of specialized entities, when applicable. Any non-sworn member who receives such information should ensure that it is passed on to a deputy in a timely manner.

If the suspicious activity is not directly related to a reportable crime, the member should prepare a SAR and include information about the involved parties and the circumstances of the incident. If, during any investigation a deputy becomes aware of suspicious activity that is unrelated to the current investigation, the information should be documented separately in a SAR and not included in the original incident report. The report number of the original incident should be included in the SAR as a cross reference. A SAR should be processed as any other incident report.

432.5 HANDLING INFORMATION

The Records Division will forward copies of SARs, in a timely manner, to:

- The Investigation Division supervisor.
- The Crime Analysis unit.
- Other authorized designees.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Procedures for Emergency and Temporary Custody Orders

433.1 PROCEDURES FOR EMERGENCY AND TEMPORARY CUSTODY ORDERS

1. If the individual is taken into custody pursuant to VA Code §37.2-808, the deputy shall request the Emergency Communication Center to contact the Rappahannock Rapidan Community Services Board (RRCSB) as soon as practical.The RRCSB has a Crisis Intervention Team Assessment Center (CITAC) located in Culpeper County, Virginia which may be utilized for the purpose of completing mental health evaluations. The use of the CITAC satisfies statutory requirements.
    (a) Any person taken into emergency custody pursuant to VA Code §37.2-808 shall be given a written summary of the emergency custody procedures and the statutory protections associated with those procedures. This written documentation is provided with the court order (Form DC-4050).
2. Arraignments will be made between RRCSB and the Sheriff's Office as to the most appropriate location for the evaluation.
3. Upon completion ofthe psychological assessment, the RRCSB evaluator may take the following steps:
    (a) The evaluator may petition the magistrate for a Temporary Detention Order (TDO) to place the individual in a designated mental health facility.
    (b) The evaluator may elect not to request a Temporary Detention Order leaving the deputy to release the detainee, or release the detainee to a relative or other responsible person.
        (a) In this event, the evaluator is required to notify the person who initiated emergency custody if present, or the on-site physician of their recommendation.If the deputy or person who caused initiation of emergency custody disagrees with the evaluator's recommendation the CSB will facilitate communication between the person or deputy and the Magistrate as soon as practical and prior to the expiration of the emergency custody period.The magistrate after consideration of all information and recommendations will make a final determination regarding the issuance of a Temporary Detention Order.
4. Temporary Detention Order is issued by the magistrate, or other judicial officer, the deputy will take custody of the subject and transport them to the designated facility.
5. If medical attention is needed prior to admittance to the mental health facility denoted on the Temporary Detention Order, the individual will be first sent to a hospital to be evaluated and treated as necessary. The transporting deputy will remain with the individual until transport is made to the final destination noted on the TDO.
6. The magistrate or judicial officer shall specify on the Temporary Detention Order the law enforcement agency responsible for the transport. The jurisdiction in which the individual resides will be responsible for transport and execution of the Temporary

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Detention Order. However, if the jurisdiction in which the individual resides is more than 50 miles from the nearest boundary, this Office will provide transportation and execute the order per VA Code §37.2-810.

7. If the deputy encounters any difficulty with any step of this process, the shift supervisor shall be contacted for guidance and direction.

8. If a Temporary Detention Order is not served within 24 hours of its issuance, or within a shorter period as specified in the order, the order shall be void and shall be returned unexecuted to the Magistrate or judicial officer who issued the order.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Service of Court Documents

434.1 PURPOSE AND SCOPE

This policy provides guidelines for serving court documents to parties in civil matters.

This policy does not apply to the service of court orders as provided in the Domestic or Family Violence Policy.

434.2 POLICY

The Madison County Sheriff's Office will deliver court documents such as subpoenas or court orders with efficiency and due care. The Department will give higher priority to the service of court orders in cases when the Department reasonably believes delay may impact a person's safety.

434.3 RESPONSIBILITIES

Requests that the Madison County Sheriff's Office serve court documents should be forwarded to the Records Manager.

434.3.1 RECORDSHEAD RESPONSIBILITIES

The Records Manager is responsible for developing procedures to ensure:

(a) Court documents received for service are logged, dated, and time stamped.

(b) A service application request form is received from the person requesting service that includes:

1. The date service is due.
2. Whether substitute service is authorized by the requestor.
3. Risk-related information such as the subject's prior acts of violence, and the presence of aggressive dogs, drugs, or other hazardous substances.

(c) Inquiries are made in law enforcement records management systems to determine if there are additional entries that would impact deputy safety when serving the papers. Proper notations should be entered on or attached to the service application request form.

(d) A fee schedule is maintained and applicable fees are collected. No fees shall be required when fees have been waived by a court or are prohibited by statute.

(e) A schedule is maintained with the number of copies of each type document the Department requires when a person requests service by the Department.

(f) Data entry regarding the service is made in a timely fashion. This includes data entry regarding the status of the service (e.g., served, attempted, returned), if appropriate.

(g) Court documents and accompanying service application request forms are forwarded to the Administration Division Supervisor for service.

(h) The court and person requesting service are promptly notified that service has been made or that attempts at service were unsuccessful. Returns of service or

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

documentation related to failure of service for out-of-county courts may be returned by mail to the person from whom it was received.

(i) The Department maintains a record that contains a list of all court documents received for service, including:

1. The date and time received.
2. Department tracking method.
3. The type of court document (e.g., civil subpoena, civil summons) and any identifying document number (e.g., docket number, warrant number).
4. The source of any document.
5. The names of the parties to the action.
6. The name and address of the person to be served unless confidential under law.
7. Method of service.
8. The date, time, and location of service or attempts of service.
9. The number and manner of attempts to serve.
10. Date and reason for non-service, if applicable.
11. The deputy assigned to serve the document and date of assignment.

(j) The Department periodically confers with applicable courts regarding the service of documents by the Department and any relevant court procedural changes or possible areas of concern or improvement that need to be addressed, as appropriate.

(k) All property acquired through civil process is properly accounted for by the Property and Evidence Section in department records and is disposed of only pursuant to legal authority (see also the Property and Evidence Section and the Asset Forfeiture policies).

434.3.2 DIVISIONADMIN DIVISIONCOMMANDER RESPONSIBILITIES

The Administration Division Supervisor is responsible for tracking requests for service received and deputies assigned to such requests to ensure service efforts are diligently made.

Upon receipt of the service application request form and court documents for service, the Administration Division Supervisor should assign service to a deputy. Court documents reasonably known to be related to a person's immediate safety should be served as soon as practicable. Any reasonably known information related to a heightened risk in the service should be addressed and communicated to the department member assigned to serve the documents.

The Administration Division Supervisor will send the completed documentation of service back to the Records Manager to ensure timely notification to the court.

The Administration Division Supervisor will also ensure that sufficient documentation related to the service and attempted service of court documents has occurred.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

The Administration Division Supervisor will ensure that orders for civil arrest or for writs involving the seizure of real or personal property are executed only by certified law enforcement officers.

434.3.3 OFFICER_DEPUTY RESPONSIBILITIES

Deputies assigned to serve court documents shall do so diligently and with due regard for privacy and property rights.

If service of a court order is not immediately possible, deputies are expected to make reasonable inquiries and investigative actions to complete the service. This may include using the following resources to locate persons:

(a) National Motor Vehicle Title Information System

(b) Public records databases and other commercial web-based sources used to find people (skip tracing tools)

(c) Relevant court records and contact information for parties

Deputies are required to complete and submit to the Administration Division Supervisor a return of service for each document served or attempted to be served.

Deputies are expected to complete and submit a report any time there is reasonable suspicion to believe a person is attempting to evade service or is being assisted by another person to avoid service.

Deputies shall not give legal advice or express opinions as to the merit of civil issues.

Deputies shall document all court documents served or attempted to be served. The documentation should include the address where service was attempted, the date and time of attempted service, any reasons or circumstances why service was unsuccessful, the date and time of service, the name of the person served and description of the service, and the mileage used for each service or service attempt.

434.4 OFFICER_DEPUTY SAFETY

Members should always review risk-related information in the service application request form prior to service. Members may contact the requestor with any questions related to information on the form that indicate an unusual risk to safety. Members should notify a supervisor if they identify any particular safety concerns that have not been addressed.

Members may consider requesting assistance from another deputy and/or avoiding confrontation at a residence or business by contacting the party and requesting to meet at a location that may pose a lower risk.

434.5 CANCELED SERVICE

Any member of the Department who becomes aware of the cancellation of court document service request should promptly inform the Administration Division Supervisor. The Administration Division Supervisor should promptly notify the assigned deputy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Service of Court Documents

434.6 PERSONAL SERVICE

All service should be made by handing a copy of the document directly to the person to whom the document is directed.

434.7 SUBSTITUTE SERVICE

Substitute service may be made by delivering a copy to any person found at the defendant's usual place of residence who is a family member and who is 16 years of age or older or as otherwise provided in Va. Code § 8.01-296.

434.8 SERVICE OF SPECIFIC DOCUMENTS

Members of this department may be called upon to serve notices, orders, and other documents prescribed by law, regular on their face, and issued by a competent authority. The Department shall develop and maintain detailed operational procedures on (Va. Code § 8.01-293 et seq.):

(a) Subpoena service.

(b) Civil writs and court orders such as legal papers other than original process.

(c) Jurisdictional issues.

These procedures should be followed by all members during the performance of the related task.

434.9 PROPERTY DISPOSITION

[Insert your agency's specific procedures consistent with standard OPR.12.03 requirements – see the Guide Sheet for additional guidance.]

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Court Security Policy

435.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the physical security and safety of department court facilities.

435.2 POLICY

It is the policy of the Madison County Sheriff's Office to provide for the physical security and safety of court facilities under department control using available resources to enhance the safety of the public and department members.

The Madison County Sheriff's Office respects the rights of people to access public buildings. It is the policy of this department not to unreasonably interfere with, harass, intimidate, or discriminate against persons engaged in the lawful exercise of their rights, while preserving the peace, protecting life, and preventing the destruction of property.

435.3 FUNCTION

Members are responsible for ensuring that all court facilities remain secure from unauthorized access at all times. All exterior doors should remain closed and locked at all times, unless there are secondary barriers or a member is present to prevent unauthorized access. All persons entering the court facility are subject to search.

The Sheriff shall assign a Division Supervisor the responsibility for administering and managing the court security function of the Madison County Sheriff's Office.

Department members should apply the following guidelines whenever practicable.

435.3.1 PUBLIC ACCESS AREAS

Public access to court facilities should only be permitted during established business hours and only when staffing is available to adequately monitor the movement of persons within the facility and to restrict access to nonpublic and secure areas. The court facility should have a designated entry area and established procedures for screening users of the facility for weapons and contraband.

435.3.2 FACILITY ACCESS CONTROL

An entry control process, including physical barriers should exist at each court facility, including those with public access. All persons entering the court facility should be screened for weapons at the time of entry. There may be varying degrees of access established with different access and escort requirements. Access categories may include but are not limited to:

(a) Employees.

(b) Judiciary.

(c) On-duty law enforcement.

(d) Emergency services.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(e) Contractors and/or vendors.

(f) Members of the public.

For the purposes of this policy, facility security includes but is not limited to:

(a) Interior and exterior doors.

(b) Windows and lighting.

(c) Emergency power, fire/smoke detection, and suppression equipment.

(d) All types of alarms.

(e) Key control.

(f) Secure areas.

(g) Circulation patterns.

(h) Communications.

(i) Restricted areas.

(j) Access for people with disabilities.

435.3.3 EQUIPMENT

All equipment that is property of the Madison County Sheriff's Office shall be maintained according to the Department-Owned and Personal Property Policy. For the purposes of this policy, department-owned court security equipment includes but is not limited to:

(a) Magnetometers.

(b) Alarms.

(c) Medical supplies.

(d) Fire suppression equipment.

(e) Restraining devices.

(f) Weapons.

(g) Communications equipment.

[Insert your guidelines consistent with standard OPR.11.05 – see the Guide Sheet for additional guidance.]

435.3.4 FACILITY SURVEY

The Madison County Sheriff's Office shall develop and implement a court facility security management plan. The court facility security management plan should be established pursuant to the results of a site survey of the court facility. The site survey should be conducted every three years.

The court facility security management plan should include but is not limited to:

(a) Emergencies (e.g., fire, medical, hostage, bomb, disaster, prisoner escape).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) High-risk and/or high-profile trials.

(c) Weapons.

(d) Use of restraining devices.

(e) Detainee movement and circulation patterns.

(f) Lockdown.

(g) Evacuation.

[Insert your information consistent with standard OPR.11.01 requirements – see the Guide Sheet for additional guidance.]

435.3.5 WEAPONS

The Madison County Sheriff's Office should ensure that weapons are excluded from the court facility, unless carried or maintained by those individuals who are authorized by law or as required for facility security. Notice that weapons shall not be possessed or brought into the court facility shall be posted conspicuously at each public entrance to each courthouse or other building containing a court facility.

Lockboxes should be available for the safe, secure, and convenient storage of weapons at the court facility. Persons storing weapons at a facility shall be provided a receipt for the firearm. Procedures for the safe receipt, handling, storage, and return of weapons should be implemented.

435.3.6 PRISONER RESTRAINTS

The use of restraints in the court facility by deputies shall be in accordance with the Handcuffing and Restraints, Temporary Custody of Adults, and Temporary Custody of Juveniles policies.

435.3.7 COURTROOMS

Courtrooms under the control of the Madison County Sheriff's Office:

(a) Should be equipped with duress alarms that terminate in an area where rapid response can be made by members of the Madison County Sheriff's Office.

(b) Shall be equipped with at least one means of external voice communication.

(c) Shall have a documented search conducted at the beginning and end of the court day.

435.4 TRAINING

The Training Supervisor should develop a training plan for all members assigned to the court facility.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Chapter 5 - Traffic Operations

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Traffic

500.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for improving public safety through education and enforcement of traffic-related laws.

500.2 POLICY

It is the policy of the Madison County Sheriff's Office to educate the public on traffic-related issues and to enforce traffic laws. The efforts of the Department will be driven by such factors as the location and/or number of traffic accidents, citizen complaints, traffic volume, traffic conditions and other traffic-related needs. The ultimate goal of traffic law enforcement and education is to increase public safety.

500.3 DEPLOYMENT

Enforcement efforts may include such techniques as geographic/temporal assignment of department members and equipment, the establishment of preventive patrols to deal with specific categories of unlawful driving and a variety of educational activities. These activities should incorporate methods that are suitable to the situation; timed to events, seasons, past traffic problems or locations; and, whenever practicable, preceded by enforcement activities.

Several factors will be considered in the development of deployment schedules for department members. State and local data on traffic accidents are a valuable resource. Factors for analysis include, but are not limited to:

- Location.
- Time.
- Day.
- Violation factors.
- Requests from the public.
- Construction zones.
- School zones.
- Special events.

Department members assigned to uniformed patrol or traffic enforcement functions will emphasize the enforcement of violations that contribute to traffic accidents, and also will consider the hours and locations where traffic accidents tend to occur. Members will take directed enforcement action on request, and random enforcement action when appropriate. Members shall maintain high visibility while working general enforcement, especially in areas where traffic accidents frequently occur.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

500.4 ENFORCEMENT

Traffic enforcement will be consistent with applicable Code of Virginia laws and take into account the degree and severity of the violation committed to include:

(a) Driving under the influence of alcohol/drugs (see the Impaired Driving Policy).

(b) Operating a vehicle after driving privileges have been suspended or revoked (see the Suspended or Revoked Licenses section of this policy).

(c) Speed violations.

(d) Other hazardous violations.

(e) Off-road vehicle violations.

(f) Equipment violations.

(g) Public carrier/commercial vehicle violations.

(h) Violations committed by juveniles.

(i) Violations committed by nonresidents (out of area and/or state).

(j) Violations resulting in traffic accidents (see the Traffic Accidents Policy).

(k) Pedestrian and/or bicycle violations.

(l) Legislators.

(m) Military personnel.

This department does not establish ticket quotas. The number of arrests made or citations issued by any member shall not be used as the sole criterion for evaluating member overall performance (Va. Code § 2.2-5516; Va. Code § 15.2-1609.11; Va. Code § 15.2-1710.1).

Several methods are effective in the reduction of traffic accidents.

500.4.1 WARNINGS

Warnings are a non-punitive option that may be considered by the member when circumstances warrant, such as when a minor violation was inadvertent.

500.4.2 SUMMONS

A summons should be issued when a member believes it is appropriate. When issuing a summons for a traffic violation, it is essential that the rights and requirements imposed on motorists be fully explained. At a minimum, motorists should be provided with (Va. Code § 46.2-388):

(a) An explanation of the violation or charge.

(b) The amount of the fine that may be assessed for the violation or charge when such fine is prepayable.

(c) The court appearance date and procedure, including the optional or mandatory appearance by the motorist.

(d) A notice of whether the motorist can enter a plea and pay the fine by mail or at the court.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(e) The consequences of a failure to timely pay or contest the charge.

500.4.3 PHYSICAL ARREST

Physical arrest can be made on a number of criminal traffic offenses. These cases usually deal with but are not limited to:

(a) Involuntary manslaughter (Va. Code § 18.2-36.1).

(b) Felony and misdemeanor driving under the influence (DUI) of alcohol or drugs (Va. Code § 18.2-270).

(c) Felony or misdemeanor hit-and-run (Va. Code § 46.2-894).

(d) DUI with accident (Va. Code § 19.2-81).

(e) Reckless driving that results in the death of another while driving with a suspended driver's license (Va. Code § 46.2-868).

(f) Racing a vehicle in violation of Va. Code § 46.2-865 that results in serious bodily injury or death to another person (Va. Code § 46.2-865.1).

500.5 SUSPENDED OR REVOKED LICENSES

If a deputy contacts a traffic violator who is also driving on a suspended or revoked license, the deputy should issue a traffic citation or make an arrest as appropriate (Va. Code § 46.2-301).

500.6 HIGH-VISIBILITY VESTS

The Department has provided American National Standards Institute (ANSI) Class II high-visibility vests to increase the visibility of department members who may be exposed to hazards presented by passing traffic or by maneuvering or operating vehicles, machinery and equipment (23 CFR 655.601).

500.6.1 REQUIRED USE

Except when working in a potentially adversarial or confrontational role, such as during vehicle stops, high-visibility vests should be worn when increased visibility would improve the safety of the department member or when the member will be exposed to the hazards of passing traffic or will be maneuvering or operating vehicles, machinery and equipment.

Examples of when high-visibility vests should be worn include traffic control duties, traffic accident investigations, lane closures and disaster scenes.

When emergency conditions preclude the immediate donning of the vest, members should retrieve and wear the vest as soon as conditions reasonably permit.

Use of the vests shall also be mandatory when directed by a supervisor.

500.6.2 CARE AND STORAGE

High-visibility vests are issued to all personnel and shall be maintained in each patrol and investigation vehicle. Before going into service, each member shall ensure that a serviceable high-visibility vest is available.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

A supply of high-visibility vests will be maintained and made available for replacement of damaged or unserviceable vests. The Training Supervisor should be promptly notified whenever the supply of vests needs replenishing.

500.7 HAZARDOUS CONDITIONS

Deputies encountering hazardous road conditions should assess the severity of the hazard and take appropriate action including, but not limited to:

(a) Notifying the County department responsible for maintaining that section of the road.

(b) Removing the hazard from the roadway if it is reasonably safe to do so.

(c) Placing a warning device around the hazard to warn oncoming traffic.

(d) When practicable and safe to do so, positioning a patrol car in front of the hazard to warn oncoming traffic and direct the traffic around the hazard.

500.8 VEHICLE CHECKPOINTS

The Patrol Division may establish guidelines for roadside vehicle checkpoints based upon reasonable criteria (e.g., holidays, traffic injuries or fatalities, community requests). Operational decisions should be made by supervising deputies. Guidelines for checkpoints should include, but are not limited to:

(a) Reasonable location and duration.

(b) Neutral criteria for stopping motorists.

(c) Clear indicators of the official nature of the checkpoint.

(d) Clearly identified deputies and equipment.

(e) Adequate safety precautions.

(f) Minimal detention of motorists.

(g) Advance public notice.

500.8.1 CHECKPOINT IMPLEMENTATION

The following procedures should be used by the supervisor assigned to a checkpoint operation when implementing a checkpoint:

(a) Establish the goal of the checkpoint, (e.g., DUI detection, Seatbelt violations.)

(b) Establish and operational plan that satisfies the guidelines as established by the Patrol Commander.

(c) Assign and notify the deputies chosen to conduct the checkpoint.

(d) Conduct an operational briefing prior to activation, communicate the operational plan and checkpoint goal.

(e) Activate the checkpoint.

(f) Track all contact and traffic that was not stopped.

(g) Conduct an after-action debriefing when the checkpoint is concluded.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(h) Generate an after-action report detailing the contacts, arrests, contraband found, areas for improvement and successes.

500.9 TRAFFIC STOPS

Deputies should perform traffic stops only when there is an articulable reason to do so. The safety of the deputy, the driver of the vehicle and the public shall be considered prior to conducting a traffic stop.

Traffic stops should be performed by a uniformed on-duty deputy.

Deputies initiating a traffic stop shall follow department-approved safety procedures including, but not limited to:

(a) If so equipped, activating the Mobile Audio Video System.

(b) Contacting the Dispatch Center regarding the location, vehicle description and registration, and occupants prior to making the stop.

(c) Activating the emergency lights and siren.

(d) Escorting the vehicle to a tactically safe location to conduct the stop.

(e) Positioning the department vehicle to maximize deputy safety.

(f) Approaching the vehicle and interacting with the occupants in accordance with department-approved procedures.

(g) Calling for backup when warranted.

500.10 TRAFFIC CONTROL

Members of the Madison County Sheriff's Office may control traffic using both department-approved temporary traffic control devices and also uniform hand signals and gestures for manual traffic direction:

(a) At public events.

(b) At the scene of a traffic collision.

(c) At the scene of a fire or other emergency.

(d) During periods of adverse road and/or weather conditions.

(e) When circumstances warrant the manual operation of traffic control devices.

(f) As required by other road or traffic conditions.

500.11 VEHICLE ESCORT SERVICES

Vehicle escort services are generally not performed. All requests for escort services should be approved by the Sheriff.

If a request is granted, the Patrol Commander should be responsible for:

(a) Identify the required department resources.

(b) Coordinate with outside agencies.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) Identify safety and security risks.

(d) Take reasonable precautions to ensure public safety.

Only vehicles equipped with emergency lights and sirens should be used to provide escort services.

Requests for escort for medical transport or civilian vehicles should be in accordance with the specifications in the Medical Aid and Response Policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Traffic Accidents

501.1 PURPOSE AND SCOPE

This policy provides guidelines for responding to and investigating traffic accidents.

501.2 POLICY

It is the policy of the Madison County Sheriff's Office to respond to traffic accidents and render or summon aid to injured victims as needed. The Department will investigate and prepare reports according to the established minimum reporting requirements with the goal of reducing the occurrence of accidents by attempting to identify the cause of the accident and through enforcing applicable laws. Unless restricted by law, traffic accident reports will be made available to the public upon request.

501.3 RESPONSE

Upon arriving at the scene, the responding member should assess the need for additional resources and summon assistance as appropriate. Generally, the member initially dispatched to the scene will be responsible for the investigation and report, if required, unless responsibility is reassigned by a supervisor.

A supervisor should be called to the scene when the incident:

(a) Is within the jurisdiction of this department and there is:

1. A life-threatening injury.
2. A fatality.
3. A County vehicle involved.
4. A County official or employee involved.
5. Involvement of an on- or off-duty member of this department.

(b) Is within another jurisdiction and there is:

1. A County of Madison County, Virginia vehicle involved.
2. A County of Madison County, Virginia official involved.
3. Involvement of an on-duty member of this department.

501.3.1 MEMBER RESPONSIBILITIES

Upon arriving at the scene, the responding member should consider and appropriately address:

(a) Traffic direction and control.

(b) Proper placement of emergency vehicles, cones, roadway flares, or other devices, if available, to provide protection for members, the public, and the scene.

(c) First aid for any injured parties if it can be done safely.

(d) The potential for involvement of hazardous materials.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(e) The need for additional support as necessary (e.g., traffic control, emergency medical services, fire department, hazardous materials response, tow vehicles).

(f) Any disturbance between involved parties.

(g) Clearance and cleanup of the roadway.

(h) Protection of the accident scene for evidence preservation when required.

501.4 NOTIFICATION

If a traffic accident involves a life-threatening injury or fatality, the responding deputy shall notify the Virginia State Police. If the VSP is unavailable, the Patrol Commander shall be notified, and the Patrol Division will handle the incident.

501.4.1 NOTIFICATION OF FAMILY

In the event of a life-threatening injury or fatality, the agency responsible for the incident should ensure notification of the victim's immediate family or coordinate such notification with the Medical Examiner, department chaplain or another suitable person. Notification should be made as soon as practicable following positive identification of the victim (Va. Code § 32.1-309.1).

The identity of any person seriously injured or deceased in a traffic accident should not be released until notification is made to the victim's immediate family.

501.5 MINIMUM REPORTING REQUIREMENTS

An accident report shall be taken when:

(a) A fatality, any injury (including complaint of pain), driving under the influence or hit-and-run is involved (Va. Code § 46.2-894).

(b) The accident results in a collision with an unattended vehicle and/or damage to property other than a vehicle and the owner of that vehicle or property cannot be located (Va. Code § 46.2-896).

(c) An on-duty member of the County of Madison County, Virginia is involved.

(d) The accident results in any damage to any County-owned or leased vehicle.

(e) The accident involves any other public agency driver or vehicle.

(f) There is damage to public property.

(g) There is damage to any vehicle to the extent that towing is required.

(h) There is property damage of at least $1,500 (Va. Code § 46.2-373).

(i) Prosecution or follow-up investigation is contemplated.

(j) Directed by a supervisor.

501.5.1 PRIVATE PROPERTY

Generally, reports should be taken regardless of whether the traffic accident occurs on private or public property (Va. Code § 46.2-899).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

501.5.2 COUNTY VEHICLE INVOLVED

A traffic accident report shall be taken when a County vehicle is involved in a traffic accident that results in property damage or injury.

A general information report may be taken in lieu of a traffic accident report at the direction of a supervisor when the incident occurs entirely on private property or does not involve another vehicle.

Whenever there is damage to a County vehicle, a vehicle damage report shall be completed and forwarded to the appropriate Division Supervisor. The traffic investigator or supervisor at the scene should determine what photographs should be taken of the scene and the vehicle damage.

501.5.3 INJURED ANIMALS

Department members should refer to the Animal Control Policy when a traffic accident involves the disposition of an injured animal.

501.6 INVESTIGATION

When a traffic accident meets minimum reporting requirements, the investigation should include, at a minimum:

(a) Identification and interview of all involved parties.

(b) Identification and interview of any witnesses.

(c) A determination of whether a violation of law has occurred and the appropriate enforcement action.

(d) Identification and protection of items of apparent evidentiary value.

(e) Documentation of the incident as necessary (e.g., statements, measurements, photographs, collection of evidence, reporting) on the appropriate forms.

501.6.1 INVESTIGATION BY OUTSIDE LAW ENFORCEMENT AGENCY

The Patrol Commander or on-duty Shift Supervisor should request that the Virginia State Police (VSP) or another outside law enforcement agency investigate and complete a traffic accident investigation when a life-threatening injury or fatal traffic accident occurs within the jurisdiction of the Madison County Sheriff's Office and involves:

(a) An on- or off-duty member of the Department.

1. The involved member shall complete the department traffic accident form. If the member is unable to complete the form, the supervisor shall complete it.

(b) An on- or off-duty official or employee of the County of Madison County, Virginia.

Department members shall promptly notify a supervisor when any department vehicle is involved in a traffic accident. The accident investigation and report shall be completed by the agency having jurisdiction.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

501.7 ENFORCEMENT ACTION

After a thorough investigation in which physical evidence or independent witness statements indicate that a violation of a traffic law contributed to the accident, authorized members should issue a summons or arrest the offending driver, as appropriate.

More serious violations, such as driving under the influence of drugs or alcohol, vehicular manslaughter or other felonies, shall be enforced. If a driver who is subject to enforcement action is admitted to a hospital, a supervisor shall be contacted to determine the best enforcement option.

501.8 REPORTS

Department members shall utilize forms approved by the Department of Motor Vehicles as required for the reporting of traffic accidents. All such reports shall be forwarded to the Traffic Records Electronic Data System (TREDS) manager for approval and filing (Va. Code § 46.2-374).

Traffic accident reports shall include (Va. Code § 46.2-373):

(a) The name or names of the insurance carrier or the insurance agent of the automobile liability policy on each vehicle involved in the accident.

(b) The speed of each vehicle involved in the accident.

(c) The types of vehicles involved in all accidents between passenger vehicles and vehicles or combinations of vehicles used to transport property.

(d) Whether any trucks involved in such accidents were covered or uncovered.

501.8.1 REPORT MODIFICATION

A change or modification of a written report that alters a material fact in the report may be made only by the member who prepared the report, and only prior to its approval and distribution. Once a report has been approved and distributed, corrections shall only be made by way of a written supplemental report. A written supplemental report may be made by any authorized member.

501.8.2 PATROL COMMANDER RESPONSIBILITIES

The responsibilities of the Patrol Commander include, but are not limited to:

(a) Ensuring the monthly and quarterly reports on traffic accident information and statistics are forwarded to the Patrol Division Supervisor or other persons as required.

(b) Ensuring that the accident report is filed with the VSP within 24 hours after the investigation is complete (Va. Code § 46.2-373).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Vehicle Towing

502.1 PURPOSE AND SCOPE

This policy provides guidance related to vehicle towing. Nothing in this policy shall require a member of this department to tow a vehicle.

502.2 POLICY

The Madison County Sheriff's Office will tow vehicles when appropriate and in accordance with the law.

502.3 REMOVAL OF VEHICLES DUE TO HAZARD

When a vehicle should be towed because it presents a hazard, the owner or operator should arrange for the towing. Department members may assist by communicating requests through the Dispatch Center to expedite the process.

If the owner or operator is unable to arrange for towing and the vehicle presents a hazard, the vehicle may be towed at the direction of the department member (Va. Code § 46.2-1209; Va. Code § 46.2-1210; Va. Code § 46.2-1211; Va. Code § 46.2-1212; Va. Code § 46.2-1212.1; Va. Code § 46.2-1213).

Vehicles that are not the property of the County should not be driven by department members unless it is necessary to move the vehicle a short distance to eliminate a hazard, prevent the obstruction of a fire hydrant or comply with posted signs.

502.4 ARREST SCENES

Whenever the owner or operator of a vehicle is arrested, the arresting deputy should provide reasonable safekeeping by leaving the vehicle secured and lawfully parked at the scene or, when appropriate, by having the vehicle towed, such as when the vehicle presents a traffic hazard or the vehicle would be in jeopardy of theft or damage if left at the scene.

Deputies are not required to investigate whether alternatives to towing a vehicle exist after an arrest. However, a vehicle should not be towed if reasonable alternatives exist. When considering whether to leave a vehicle at the scene, deputies should take into consideration public safety as well as the reasonable safety of the vehicle and its contents (Va. Code § 19.2-80.1).

The following are examples of situations where a vehicle should not be towed:

- The vehicle can be legally parked, left in a reasonably secure and safe location and is not needed as evidence.
- The vehicle is parked on private property, on which the arrestee or owner is legally residing, or the property owner does not object to the vehicle being parked at that location.
- The arrestee or owner of the vehicle requests that it be released to a person who is present, willing and able to legally take control of the vehicle.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

- The vehicle is legally parked and the arrestee or owner requests that it be left at the scene. In such cases the requester should be informed that the Department will not be responsible for theft or damages.

502.5 VEHICLES RELATED TO CRIMINAL INVESTIGATIONS

Deputies should tow vehicles that are needed for the furtherance of an investigation or prosecution of a case, or that are otherwise appropriate for seizure as evidence. Deputies should make reasonable efforts to return a recovered stolen vehicle to its owner rather than have it towed, so long as the vehicle is not needed for evidence.

502.6 RECORDS

Records Division members shall ensure that pertinent data regarding a towed vehicle is promptly entered into the Virginia Department of Motor Vehicles (DMV) database (Va. Code § 46.2-1209).

502.6.1 VEHICLE STORAGE REPORT

Department members towing a vehicle shall complete a vehicle tow report. The report should be submitted to the Records Division as soon as practicable after the vehicle is towed.

502.6.2 NOTICE OF TOW

When a vehicle is removed from public or private property by a member of the Madison County Sheriff's Office, the member shall contact the DMV and all registered owners, and provide them notice of towing (Va. Code § 46.2-1209; Va. Code § 46.2-1211).

The member shall provide to the registered owners the following information:

(a) The name, address and telephone number of the Madison County Sheriff's Office.

(b) The location where the vehicle is stored.

(c) A description of the vehicle, including:

1. Color.
2. Manufacturer year.
3. Make and model.
4. License plate number and/or Vehicle Identification Number (VIN).
5. Mileage.

(d) The authority and purpose for the removal of the vehicle.

(e) An explanation of the procedure for release of the vehicle and for obtaining a vehicle tow hearing.

502.7 TOWING SERVICES

The County of Madison County, Virginia may, by ordinance, regulate the selection of one or more businesses to act as the official tow services of Madison County, Virginia (Va. Code § 46.2-1217).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Members shall not show preference among towing services that have been authorized for use by the Department. If more than one towing service has been awarded contracts, they shall be placed on a rotation list.

502.8 VEHICLE INVENTORY

The contents of all vehicles towed at the request of department members shall be inventoried and listed on the inventory report. When reasonably practicable, photographs may be taken to assist in the inventory.

(a) An inventory of personal property and the contents of open containers will be conducted throughout the passenger and engine compartments of the vehicle including, but not limited to, any unlocked glove box, other accessible areas under or within the dashboard area, any pockets in the doors or in the back of the front seat, in any console between the seats, under any floor mats and under the seats.

(b) In addition to the passenger and engine compartments as described above, an inventory of personal property and the contents of open containers will also be conducted in any other type of unlocked compartments that are a part of the vehicle, including unlocked vehicle trunks and unlocked car top containers.

(c) Any locked compartments including, but not limited to, locked glove compartments, locked vehicle trunks, locked hatchbacks and locked car-top containers should be inventoried, provided the keys are available and released with the vehicle to the third-party towing company or an unlocking mechanism for such compartment is available within the vehicle.

(d) Closed containers located either within the vehicle or any of the vehicle's compartments will not be opened for inventory purposes except for the following: wallets, purses, coin purses, fanny packs, personal organizers, briefcases or other closed containers designed for carrying money, small valuables or hazardous materials.

Members should ask the occupants whether the vehicle contains any valuables or hazardous materials. Responses should be noted in the inventory report. If the occupant acknowledges that any closed container contains valuables or a hazardous material, the container shall be opened and inventoried. When practicable and appropriate, such items should be removed from the vehicle and given to the owner, or booked into property for safekeeping.

Any cash, jewelry or other small valuables located during the inventory process will be held for safekeeping, in accordance with the Property and Evidence Section Policy. A copy of the property receipt should be given to the person in control of the vehicle or, if that person is not present, left in the vehicle.

A copy of the vehicle inventory will be given to the tow truck operator.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

These inventory procedures are for the purpose of protecting the vehicle owner's property, providing for the safety of department members and protecting the Department against fraudulent claims of lost, stolen or damaged property.

Towing a vehicle in order to perform an inventory should not be used as a pretext for an evidence search. Nothing in this policy prevents the towing of a vehicle that would occur for reasons independent of any suspicion that the vehicle may contain evidence if it is otherwise justified by law or this policy.

502.9 SECURITY OF VEHICLES AND RETRIEVAL OF PROPERTY

If the search of a vehicle leaves the vehicle or any property contained therein vulnerable to unauthorized entry, theft or damage, the department member conducting the search shall take such steps as are reasonably necessary to secure or protect the vehicle or property from such hazards.

Unless it would cause an unreasonable delay in towing the vehicle or create an issue of officer safety, reasonable accommodations should be made to permit the owner, operator or occupant to retrieve small items of value or personal need (e.g., cash, jewelry, cell phone, prescriptions) that are not considered evidence or contraband.

Members who become aware that a vehicle may have been towed by the Department in error should promptly advise a supervisor. Supervisors should approve, when appropriate, the release of the vehicle without requiring the owner or his/her agent to request a hearing to contest the tow.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Vehicle Tow Hearings

503.1 PURPOSE AND SCOPE

The purpose of this policy is to establish a process for vehicle tow hearings.

503.2 POLICY

When a vehicle is towed at the direction of any member of the Madison County Sheriff's Office, a hearing will be conducted upon written request filed with the Commonwealth Attorney's Office for Madison County.

503.3 HEARING OFFICER

The Madison County Commonwealth Attorney, or designee, will act as a hearing officer when the decision of a member to tow a vehicle is contested. The hearing officer in any case must be a person other than the member who directed the vehicle to be towed.

503.4 HEARING PROCESS

The registered or legal owner of the vehicle or his/her agent may request a hearing when a vehicle is towed or stored at the direction of any member of the Madison County Sheriff's Office (Va. Code § 19.2-80.1; Va. Code § 46.2-1209; Va. Code § 46.2-1211; Va. Code § 46.2-890).

The failure to request a hearing in a timely manner or to attend a scheduled hearing may be considered a waiver of and satisfaction of the hearing.

The requested hearing shall be conducted within 48 hours of the request, excluding weekends and holidays.

Any relevant evidence may be submitted and reviewed by the hearing officer to determine the validity of the tow.

Certain hearings, such as driving with a suspended or revoked license, may be reviewed by the appropriate general district court upon a petition of the driver, owner or co-owner of the vehicle (Va. Code § 46.2-301.1).

503.5 DECISION

After consideration of all the evidence, the hearing officer shall determine whether the Department has established the validity of the tow by a preponderance of the evidence.

(a) If a decision is made that reasonable grounds for the tow have been established, the hearing officer shall advise the requesting party of the decision.

(b) If a decision is made that reasonable grounds for the tow have not been established, the vehicle shall be released immediately. Towing and storage fees will be the responsibility of the Department.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Impaired Driving

504.1 PURPOSE AND SCOPE

This policy provides guidance to those department members who play a role in the detection and investigation of driving under the influence (DUI) of alcohol or drugs.

504.2 POLICY

The Madison County Sheriff's Office is committed to the safety of the roadways and the community and will pursue fair but aggressive enforcement of Virginia's impaired driving laws.

504.3 INVESTIGATIONS

Deputies should not enforce DUI laws to the exclusion of their other duties unless specifically assigned to DUI enforcement. All deputies are expected to enforce these laws with due diligence.

The Patrol Commander will develop and maintain, in consultation with the prosecuting attorney, report forms with appropriate checklists to assist investigating deputies in documenting relevant information and maximizing efficiency. Any DUI investigation will be documented using these forms. Information documented elsewhere on the form does not need to be duplicated in the report narrative. Information that should be documented includes, at a minimum:

(a) The field sobriety tests (FSTs) administered and the results.

(b) The deputy’s observations that indicate impairment on the part of the individual, and the deputy’s health-related inquiries that may help to identify any serious health concerns (e.g., diabetic shock).

(c) Sources of additional information (e.g., reporting party, witnesses) and their observations.

(d) Information about any audio and/or video recording of the individual’s driving or subsequent actions.

(e) The location and time frame of the individual’s vehicle operation and how this was determined.

(f) Any prior related convictions in Virginia or another jurisdiction.

504.4 FIELD TESTS

The Patrol Commander should identify standardized FSTs and any approved alternate tests for deputies to use when investigating violations of DUI laws.

504.4.1 PRELIMINARY BREATH TESTS

If the driver is suspected of being DUI and has failed the standardized FSTs, a preliminary breath test (PBT), if available, shall be offered. The person shall be advised of his/her right to refuse the PBT. The person may observe the process of analysis and the results of the test, if requested (Va. Code § 18.2-267).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Impaired Driving

504.5 CHEMICAL TESTS

A person, whether licensed in Virginia or not, implies consent under Virginia law to a chemical test or tests, and to providing the associated chemical sample if the person has been arrested for any of the following (or a similar ordinance) within three hours of the alleged offense (Va. Code § 18.2-268.2; Va. Code § 46.2-341.26:2):

(a) DUI (Va. Code § 18.2-266)

(b) Minor DUI (Va. Code § 18.2-266.1)

(c) Driving after license forfeiture (Va. Code § 18.2-272)

(d) Commercial vehicle DUI (Va. Code § 46.2-341.24; Va. Code § 46.2-341.31)

If a person withdraws this implied consent, or is unable to withdraw consent (e.g., the person is unconscious), the deputy should consider implied consent revoked and proceed as though the person has refused to provide a chemical sample.

The test shall be of the person's breath unless a breath test is unavailable or the person is physically unable to submit to a breath test, in which case a blood test shall be given. If there is reason to believe that the person was driving under the influence of both alcohol and drugs, or drugs alone, a blood test may be administered in addition to the breath test. Testsmust be administered within three hours of the arrest (Va. Code § 18.2-268.2).

504.5.1 STATUTORY NOTIFICATIONS

The deputy shall inform the person, prior to the test, that analysis of the reading and the results may be observed. If the equipment used produces a written printout, the person shall be given a copy (Va. Code § 18.2-268.2).

504.5.2 BREATH SAMPLES

The Patrol Commander should ensure that all devices used for the collection and analysis of breath samples are properly serviced and tested, and that a record of such service and testing is properly maintained.

Deputies who have been certified to obtain a breath sample should monitor the device for any sign of malfunction. Any anomalies or equipment failures should be noted in the appropriate report and promptly reported to the Patrol Commander (Va. Code § 18.2-268.9).

504.5.3 BLOOD SAMPLES

Only persons authorized by law to draw blood shall collect blood samples (Va. Code § 18.2-268.5). The blood draw should be witnessed by the assigned deputy. No deputy, even if properly certified, should perform this task.

Deputies should inform an arrestee that if he/she chooses to provide a blood sample, a separate sample can be collected for alternate testing. Unless medical personnel object, two samples should be collected and retained as evidence, so long as only one puncture is required.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

The blood sample shall be packaged, marked, handled, stored and transported as required by the Department of Forensic Science.

If an arrestee cannot submit to a blood draw because he/she has a bleeding disorder or has taken medication that inhibits coagulation, he/she shall not be required to take a blood test. Such inability to take a blood test shall not be considered a refusal. However, that arrestee may be required to complete another available and viable test.

504.6 REFUSALS

When an arrestee refuses to provide a chemical sample, deputies shall (Va. Code § 18.2-268.3; Va. Code § 46.2-341.26:3):

(a) Advise the arrestee of the requirement to provide a sample (Va. Code § 18.2-268.2; Va. Code § 46.2-341.26:2).

1. If the person was driving on private property, the deputy should make reasonable attempts to obtain a voluntary chemical test sample.

(b) Audio- and/or video-record the admonishment and the response when it is practicable.

(c) Document the refusal in the appropriate report.

504.6.1 STATUTORY NOTIFICATIONS UPON REFUSAL

Upon refusal to submit to a chemical test, deputies shall advise the person, using the Declaration and Acknowledgement of Refusal form, of the consequences of such refusal (Va. Code § 18.2-268.3; Va. Code § 46.2-341.26:3).

504.6.2 DEPUTY DECLARATIONS UNDER OATH

The arresting deputy shall execute the Declaration and Acknowledgement of Refusal form, under oath before a magistrate certifying (Va. Code § 18.2-268.3; Va. Code § 46.2-341.26:3):

(a) The arrestee has refused to permit breath or blood samples to be taken for testing.

(b) The deputy has read the form to the arrestee.

(c) The arrestee has still refused to provide a sample after being read the admonishment.

(d) Whether the arrestee has any prior convictions within the last 10 years.

504.6.3 BLOOD SAMPLE WITHOUT CONSENT

A blood sample may be obtained from a person who refuses to submit to a chemical test when any of the following conditions exist:

(a) A search warrant has been obtained.

(b) The deputy can articulate that exigent circumstances exist. Exigency does not exist solely because of the short time period associated with the natural dissipation of alcohol or controlled or prohibited substances in the person’s bloodstream. Exigency can be established by the existence of special facts, such as a lengthy time delay resulting from an accident investigation or medical treatment of the person.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

504.6.4 FORCED BLOOD SAMPLE

If an arrestee indicates by word or action that he/she will physically resist a blood draw, the deputy should request a supervisor to respond.

The responding supervisor should:

(a) Evaluate whether using force to obtain a blood sample is appropriate under the circumstances.

(b) Ensure that all attempts to obtain a blood sample through force cease if the person agrees to, and completes, a viable form of testing in a timely manner.

(c) Advise the person of his/her duty to provide a sample (even if this advisement was previously done by another deputy), and attempt to persuade the individual to submit to providing such a sample without physical resistance.

1. This dialogue should be recorded on audio and/or video when practicable.

(d) Ensure that the blood sample is taken in a medically approved manner.

(e) Ensure that the forced blood draw is recorded on audio and/or video when practicable.

(f) Monitor and ensure that the type and level of force applied appears reasonable under the circumstances:

1. Unless otherwise provided in a warrant, force should generally be limited to handcuffing or similar restraint methods.

2. In misdemeanor cases, if the arrestee becomes violent or more resistant, no additional force will be used and a refusal should be noted in the report.

3. In felony cases, force which reasonably appears necessary to overcome the resistance to the blood draw may be permitted.

(g) Ensure the use of force and methods used to accomplish the collection of the blood sample are documented in the related report.

If a supervisor is unavailable, deputies are expected to use sound judgment and perform the duties of a supervisor, as set forth above.

504.7 ARREST AND INVESTIGATION

Deputies may make a warrantless arrest within three hours of an alleged DUI offense, whether or not the offense was committed in the deputy’s presence (Va. Code § 19.2-81).

504.7.1 TRAFFIC ACCIDENTS

Virginia law allows deputies to make an arrest of a DUI driver involved in an accident even though the accident was not committed in his/her presence (Va. Code § 19.2-81). Deputies shall include relevant facts and circumstantial evidence that tends to show that the particular person was the driver of the vehicle.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

504.8 RECORDS DIVISION RESPONSIBILITIES

The Records Manager will ensure that all case-related records are transmitted according to current records procedures and as required by the prosecuting attorney's office.

504.9 ADMINISTRATIVE HEARINGS

The Records Manager will ensure that all appropriate reports and documents related to administrative license suspensions are reviewed and forwarded to the Virginia Department of Motor Vehicles (DMV) and entered into the Virginia Criminal Information Network (VCIN) as applicable.

Any deputy who receives notice of required attendance at an administrative license suspension hearing should promptly notify the prosecuting attorney.

A deputy called to testify at an administrative hearing should document the hearing date and the DMV file number in a supplemental report. Specific details of the hearing generally should not be included in the report unless errors, additional evidence or witnesses are identified.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Traffic and Parking Citations

505.1 PURPOSE AND SCOPE

This policy outlines the responsibilities for issuing, correcting, voiding and dismissing traffic and parking citations.

505.2 POLICY

It is the policy of the Madison County Sheriff's Office to enforce all traffic laws fairly and equally for all persons. Authorized members may issue a traffic citation, parking citation, or written or verbal warning based upon the circumstances of the contact and in the best interest of the motoring public and community safety.

505.3 RESPONSIBILITIES

The Records Division shall be responsible for the supply and accounting of all traffic and parking citations issued to members of this department. Citations will be kept in a secure location and issued to members by the Records Division staff. Members will sign for the citation books when issued or upon return of unused citations.

Members of the Madison County Sheriff's Office shall only use department-approved traffic and parking citation forms.

The Records Division should provide information to the violator including the mandatory or discretionary court appearance schedule and any prepayment information.

505.3.1 WRITTEN OR VERBAL WARNINGS

Written or verbal warnings may be issued when the department member believes it is appropriate. The Records Division should maintain information relating to traffic stops in which a written warning is issued. Written warnings are retained by this department in accordance with the established records retention schedule.

505.4 TRAFFIC CITATIONS

505.4.1 CORRECTION

When a traffic citation is issued but is in need of correction, the member issuing the citation shall submit the citation and a letter to his/her immediate supervisor requesting a specific correction. Once approved, the citation and letter shall then be forwarded to the Records Division. The Records Manager or the authorized designee shall prepare a letter of correction to the court having jurisdiction and notify the citation recipient in writing.

505.4.2 VOIDING

Voiding a traffic citation may occur when the citation has not been completed or when it is completed but not issued. All copies of the voided citation shall be presented to a supervisor for approval. The citation and copies shall then be forwarded to the Records Division.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

505.4.3 DISMISSAL

Members of this department do not have the authority to dismiss a traffic citation once it has been issued. Only the court has that authority. Any request from a recipient to dismiss a citation shall be referred to the Patrol Commander. Upon a review of the circumstances involving the issuance of the traffic citation, the Patrol Commander may request the Patrol Division Supervisor to recommend dismissal. If approved, the citation will be forwarded to the appropriate prosecutor with a request for dismissal. All recipients of traffic citations whose request for dismissal has been denied shall be referred to the appropriate court.

Prior to a court hearing, a member may submit a request for dismissal of a traffic citation to his/her supervisor. The request must be in writing and should include the reason for dismissal (i.e., in the interest of justice, prosecution is deemed inappropriate). Upon a review of the circumstances involving the issuance of the traffic citation, the supervisor may forward the request to the Patrol Division Supervisor to recommend dismissal. If approved, the citation will be forwarded to the appropriate prosecutor with a request for dismissal.

Should a member determine during a court proceeding that a traffic citation should be dismissed in the interest of justice or where prosecution is deemed inappropriate, the member may request the court to dismiss the citation. Upon such dismissal, the member shall notify his/her immediate supervisor of the circumstances surrounding the dismissal and shall complete any paperwork as directed or required, and forward it to the Patrol Division Supervisor for review.

505.4.4 DISPOSITION

The court and file copies of all traffic citations issued by members of this department shall be forwarded to the member’s immediate supervisor for review by the end of each shift. The citation copies shall then be filed with the Records Division.

Upon separation from appointment or employment with this department, all members who were issued traffic citation books shall return any unused citations to the Records Division.

505.4.5 JUVENILE CITATIONS

Completion of traffic citation forms for juveniles may vary slightly from the procedure for adults. The juvenile’s age, place of residency and the type of offense should be considered before issuing a juvenile a citation.

505.4.6 DATA COLLECTION

Each time a deputy makes a traffic stop, the deputy shall report any information as required in the Bias-Based Policing Policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Disabled Vehicles

506.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for department members who provide assistance to motorists in disabled vehicles within the primary jurisdiction of the Madison County Sheriff's Office.

506.2 POLICY

It is the policy of the Madison County Sheriff's Office to assist motorists with disabled vehicles until those vehicles are safely removed from the roadway. Members should take appropriate action to mitigate potential problems when a vehicle constitutes a traffic hazard or the safety of the motorist is a concern.

506.3 RESPONSIBILITIES

When an on-duty member of this department sees a disabled vehicle on the roadway, the member should make a reasonable effort to provide assistance. If this is not reasonably possible, the dispatcher should be advised of the location of the disabled vehicle and the need for assistance. The dispatcher should then assign another department member to respond as soon as practicable.

506.4 ASSISTANCE

In most cases, a disabled motorist will require assistance. After arrangements for assistance are made, continued involvement by department members will be contingent on the time of day, the location, the availability of department resources and the vulnerability of the disabled motorist.

506.4.1 MECHANICAL REPAIRS

Department members shall not make mechanical repairs to a disabled vehicle. The use of push bumpers, with consent of the owner, to relocate vehicles to a position of safety is not considered a mechanical repair. At their discretion, deputies may change a tire or assist a motorist in starting their engine using a jump box. Deputies shall not use their vehicles for this purpose.

506.4.2 RELOCATION OF DISABLED VEHICLES

The relocation of disabled vehicles by members of this department by pushing or pulling a vehicle should only occur when the conditions reasonably indicate that immediate movement is necessary to reduce a hazard presented by the disabled vehicle.

506.4.3 RELOCATION OF DISABLED MOTORIST

The relocation of a disabled motorist should only occur with the person’s consent and should be suggested when conditions reasonably indicate that immediate movement is necessary to mitigate a potential hazard. The department member may stay with the disabled motorist or transport him/her to a safe area to await pickup.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

506.4.4 EMERGENCY CONDITIONS

Should the disabled motorist be in jeopardy of injury or any other emergency condition is evident, the assistance response should be elevated to correspond to the circumstance.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Traffic Procedures

507.1 PURPOSE AND SCOPE

This procedure provides guidance to members in the use of department-approved traffic management methods.

507.2 TRAFFIC DIRECTION AND CONTROL

507.2.1 MANUAL TRAFFIC DIRECTION

High-visibility vests should be worn in accordance with the Traffic Policy.

Department members assigned or authorized to control traffic should use the following uniform hand gestures to perform manual traffic direction:

(a) Stopping traffic: The member should extend the arm and index finger toward and look directly at the driver to be stopped until that driver is or appears to be aware of the member's gesture. The member should then raise the pointing hand at the wrist so that the palm is toward the person to be stopped, and hold the palm in this position until the person stops. To stop traffic from both directions, the member should repeat the procedure for traffic coming from the other direction and continue to maintain the raised arm and palm toward the previously stopped traffic.

(b) Starting traffic: The member should stand with the member's shoulder and side toward the traffic to be started, extend the arm and index finger toward, and look directly at the driver to be started until that driver is or appears to be aware of the member's gesture. The member should then swing the pointing arm, with palm up, from the elbow through a vertical semicircle until the hand is adjacent to the chin. If necessary, the member should repeat until traffic begins to move. To start traffic from both directions, the member should repeat the procedure for traffic coming from the other direction.

(c) Right or left turn: The member's extended arm, index finger, and gaze should first be directed toward the driver. The member should then swing the extended arm and index finger in the direction of the driver's intended turn.

(d) Use of flashlight: A flashlight may be used to stop traffic. To stop traffic, the member should slowly swing the beam of light across the path of oncoming traffic. The beam should strike the pavement as an elongated spot of light. After the driver has stopped, the member should use hand gestures with the vehicle headlights to provide illumination.

The member should stop all traffic and address the dangerous condition with all traffic stopped.

507.2.2 ACCIDENT SCENES

Members should refer to the Traffic Accidents Policy for additional guidance.

Additional guidelines should include as appropriate:

(a) If a traffic accident results in traffic congestion, a member may request additional assistance, if available, to help with traffic control. Incidents occurring during heavy traffic periods on major streets resulting from a traffic accident and/or adverse road and

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

weather conditions may also require the use or operation of temporary traffic control devices (e.g., barriers, cones, flares, traffic signals).

1. Members should use uniform hand gestures for manual traffic direction to assist in the efficient and safe movement of vehicle and pedestrian traffic.
2. Members should coordinate traffic direction with other members at the scene, if appropriate.

(b) Traffic may be stopped, rerouted, or restricted as necessary to ensure the safety of members, victims, and uninvolved motorists.

507.2.3 CRITICAL INCIDENT SCENES

(a) Members providing traffic direction and control at critical incident scenes (e.g., fires, utility emergencies) should prevent unauthorized vehicles and pedestrians from entering the area and provide a safe arrival route for emergency vehicles.

(b) The Department should coordinate its efforts with other emergency service agencies at fires, utility emergencies, or other scenes to provide crowd control and adequate safety measures for vehicle and pedestrian traffic.

(c) Members should use temporary traffic control devices as necessary and should manually direct and control the flow of all traffic in accordance with this policy.

(d) Members should contact a supervisor if additional assistance is needed at a location for any reason.

507.2.4 HAZARDOUS ROAD CONDITIONS

Hazardous road conditions due to weather, road damage, or other emergencies should be addressed as soon as practicable.

(a) A member who locates or is assigned to investigate a hazardous road condition should use temporary traffic control devices if necessary to identify the hazard to the public, isolate it, and limit the public's ability to come into contact with or access the area.

(b) A member who locates or is assigned to investigate a hazardous condition should assess the condition and request through the Dispatch Center that notifications be made to appropriate authorities responsible for correcting the hazard. The dispatcher should document the condition and all notifications that are made.

(c) If a member needs assistance with isolating a hazard, the member may request additional members to the location.

(d) If there are any questions regarding the proper isolation of a roadway hazard, members should contact their supervisor.

1. Members should only use road flares when there is no risk of fire or explosion. Road flares should not be left unattended while burning. Any remnants left after a flare has been exhausted and allowed time to cool should be collected and disposed of properly.

(e) A member should only clear from the location under one of the following circumstances:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1. The hazardous condition has been corrected.
2. The member is relieved by an appropriate authority who will conduct the repair, and traffic direction and control services are no longer needed.
3. The member is properly relieved by another member.
4. When authorized by a supervisor.

507.2.5 MANUAL OPERATION OF TRAFFIC CONTROL DEVICES

On occasion, members may have to manually operate traffic lights or set traffic lights to flash. Only authorized members should manually operate traffic control devices with the approval of a supervisor and for the following purposes:

(a) To correct a traffic light malfunction

(b) To facilitate movement at traffic accidents or other emergencies

(c) To provide passage for a motorcade or funeral procession

(d) To alleviate congestion, particularly during planned special events

507.2.6 TEMPORARY TRAFFIC CONTROL DEVICES

Temporary traffic control devices (e.g., cones, signs, barricades) should be deployed using the procedures set forth in the most recent edition of the National Manual on Uniform Traffic Control Devices.

507.3 VEHICLE ESCORT SERVICES

Vehicle escort services are generally not performed. All requests for law enforcement escort services should be approved by the Sheriff.

If a request is granted, the Patrol Commander should be responsible for:

(a) Identifying the required department resources.

(b) Coordinating with outside agencies.

(c) Identifying safety and security risks.

(d) Taking reasonable precautions to ensure public safety.

Only vehicles equipped with emergency lights and sirens should be used to provide escort services.

Requests for escort for medical transport or civilian vehicles should be in accordance with the specifications in the Medical Aid and Response Policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Chapter 6 - Investigation Operations

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Investigation and Prosecution

600.1 PURPOSE AND SCOPE

The purpose of this policy is to set guidelines and requirements pertaining to the handling and dispositions of criminal investigations.

600.2 POLICY

It is the policy of the Madison County Sheriff's Office to investigate crimes thoroughly and with due diligence, and to evaluate and prepare criminal cases for appropriate clearance or submission to a prosecutor.

600.3 INITIAL INVESTIGATION

600.3.1 NON-SWORN MEMBER RESPONSIBILITIES

A non-sworn member assigned to any preliminary investigation is responsible for all investigative steps, except making any attempt to locate, contact or interview a suspect face-to-face or take any enforcement action. Should an initial investigation indicate that those steps are required, the assistance of a deputy shall be requested.

600.3.2 DEPUTY RESPONSIBILITIES

A deputy responsible for an initial investigation shall complete no less than the following:

(a) Make a preliminary determination of whether a crime has been committed by completing, at a minimum:
    1. An initial statement from any witnesses or complainants.
    2. A cursory examination for evidence.
    3. Documentation of any pertinent conditions, events and remarks.

(b) If information indicates a crime has occurred, the deputy shall:
    1. Preserve the scene and any evidence as required to complete the initial and follow-up investigation.
    2. Determine whether additional investigative resources (e.g., investigators or scene processing) are necessary and request assistance as required.
    3. If assistance is warranted, or if the incident is not routine, notify a supervisor or the Shift Supervisor.
    4. Make reasonable attempts to locate, identify and interview all available victims, complainants, witnesses and suspects.
    5. Collect any evidence.
    6. Take any appropriate law enforcement action.
    7. Complete and submit the appropriate reports and documentation.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) If the preliminary determination is that no crime occurred, determine what other action may be necessary and what other resources may be available, and advise the informant or complainant of this information.

600.4 CUSTODIAL INTERROGATION REQUIREMENTS

Suspects who are in custody and subjected to an interrogation shall be given the *Miranda* warning, unless an exception applies. Interview or interrogation of a juvenile shall be in accordance with the Temporary Custody of Juveniles Policy.

600.4.1 AUDIO/VIDEO RECORDINGS

A deputy conducting a custodial interrogation at the Department or in any facility where suspects may be detained shall record the entire interrogation (e.g., video with audio, just audio if video is not available) as required by law (Va. Code § 19.2-390.04).

Outside of the Department or any facility where suspects may be detained, any custodial interrogation of an individual who is suspected of having committed any violent felony offense should be recorded (audio or video with audio as available) in its entirety. Regardless of where the interrogation occurs, every reasonable effort should be made to secure functional recording equipment to accomplish such recordings.

Consideration should also be given to recording a custodial interrogation, or any investigative interview, for any other offense when it is reasonable to believe it would be appropriate and beneficial to the investigation and is otherwise allowed by law.

No recording of a custodial interrogation should be destroyed or altered without written authorization from the prosecuting attorney and the Investigation Division supervisor. Copies of recorded interrogations or interviews may be made in the same or a different format as the original recording, provided the copies are true, accurate, and complete, and are made only for authorized and legitimate law enforcement purposes. Any recordings made should be retained until the conclusion of any resulting charges and the completion of any resulting sentence (Va. Code § 19.2-390.04).

Recordings should not take the place of a thorough report and investigative interviews. Written statements from suspects should continue to be obtained when applicable.

600.4.2 INTERVIEW ROOMS

Interview room use is guided by the following:

(a) Interview rooms should be constantly monitored through visual and/or video technology of the person placed and left alone in an interview room.

(b) Members should remain in close proximity of the interview room and be available to immediately intervene on behalf of the person or Madison County Sheriff's Office as needed.

(c) Deputies should conduct a search of the interview room prior to and after each interview and search the person as necessary.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Weapons should be secured in accordance with any applicable department specifications.

(e) Access to keys and other access devices to the interview rooms should be controlled and monitored.

(f) The Training Supervisor shall ensure that all members authorized to utilize the interview rooms receive proper training.

600.5 DISCONTINUATION OF INVESTIGATIONS

The investigation of a criminal case or efforts to seek prosecution should only be discontinued if one of the following applies:

(a) All reasonable investigative efforts have been exhausted, there is no reasonable belief that the person who committed the crime can be identified and the incident has been documented appropriately.

(b) The perpetrator of a misdemeanor has been identified and a warning is the most appropriate disposition.

1. In these cases, the investigator shall document that the person was warned and why prosecution was not sought.

2. Warnings shall not be given for felony offenses or other offenses identified in this policy or by law that require an arrest or submission of a case to a prosecutor.

(c) The case has been submitted to the appropriate prosecutor but no charges have been filed. Further investigation is not reasonable nor has the prosecutor requested further investigation.

(d) The case has been submitted to the appropriate prosecutor; charges have been filed; further investigation is not reasonable, warranted or requested; and there is no need to take the suspect into custody.

(e) Suspects have been arrested, there are no other suspects, and further investigation is either not warranted or requested.

(f) Investigation has proved that a crime was not committed (see the Sexual Assault Investigations Policy for special considerations in these cases).

The Domestic or Family Violence, Child Abuse, Sexual Assault Investigations and Adult Abuse policies may also require an arrest or submittal of a case to a prosecutor.

600.6 COMPUTERS AND DIGITAL EVIDENCE

The collection, preservation, transportation and storage of computers, cell phones and other digital devices may require specialized handling to preserve the value of the related evidence. If it is anticipated that computers or similar equipment will be seized, deputies should request that computer forensic examiners assist with seizing computers and related evidence. If a forensic examiner is unavailable, deputies should take reasonable steps to prepare for such seizure and use the resources that are available.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

600.7 INVESTIGATIVE USE OF SOCIAL MEDIA AND INTERNET SOURCES

Use of social media and any other internet source to access information for the purpose of criminal investigation shall comply with applicable laws and policies regarding privacy, civil rights and civil liberties. Information gathered via the internet should only be accessed by members while on-duty and for purposes related to the mission of this department. If a member encounters information relevant to a criminal investigation while off-duty or while using his/her own equipment, the member should note the dates, times and locations of the information and report the discovery to his/her supervisor as soon as practicable. The member, or others who have been assigned to do so, should attempt to replicate the finding when on-duty and using department equipment.

Information obtained via the internet should not be archived or stored in any manner other than department-established record keeping systems (see the Records Maintenance and Release and Criminal Organizations policies).

600.7.1 ACCESS RESTRICTIONS

Information that can be accessed from any department computer, without the need of an account, password, email address, alias or other identifier (unrestricted websites), may be accessed and used for legitimate investigative purposes without supervisory approval.

Accessing information from any internet source that requires the use or creation of an account, password, email address, alias or other identifier, or the use of nongovernment IP addresses, requires supervisor approval prior to access. The supervisor will review the justification for accessing the information and consult with legal counsel as necessary to identify any policy or legal restrictions. Any such access and the supervisor approval shall be documented in the related investigative report.

Accessing information that requires the use of a third party’s account or online identifier requires supervisor approval and the consent of the third party. The consent must be voluntary and shall be documented in the related investigative report.

Information gathered from any internet source should be evaluated for its validity, authenticity, accuracy and reliability. Corroborative evidence should be sought and documented in the related investigative report.

Any information collected in furtherance of an investigation through an internet source should be documented in the related report. Documentation should include the source of information and the dates and times that the information was gathered.

600.7.2 INTERCEPTING ELECTRONIC COMMUNICATION

Intercepting social media communications in real time may be subject to federal and state wiretap laws. Deputies should seek legal counsel before any such interception.

600.8 IDENTITY THEFT

A report should be taken any time a person living within the jurisdiction of the Madison County Sheriff's Office reports that he/she has been a victim of identity theft. This includes (Va. Code § 18.2-186.3:1):

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) Taking a report, even if the location of the crime is outside the jurisdiction of this department or has not been determined.

(b) Providing the victim with the appropriate information, as set forth in the Victim and Witness Assistance Policy. Department members should encourage the individual to review the material and should assist with any questions.

A report should also be taken if a person living outside department jurisdiction reports an identity theft that may have been committed or facilitated within this jurisdiction (e.g., use of a post office box in Madison County, Virginia to facilitate the crime).

A member investigating a case of identity theft should ensure that the case is referred to the appropriate agency if it is determined that this department should not be the investigating agency (e.g., an identity theft ring working from out of state). The victim should be advised that the case is being transferred to the agency of jurisdiction. The appropriate entries should be made into any databases that have been authorized for department use and are specific to this type of investigation.

600.9 FIREARMS

Any member who seizes a firearm should make reasonable efforts to promptly identify and trace the history of the firearm and report required information to the National Tracing Center of the Bureau of Alcohol, Tobacco, Firearms and Explosives within the U.S. Department of Justice (Va. Code § 52–25.1; 19 VAC 30-115-10).

If reporting a firearm may compromise an on-going investigation, members should consult with a supervisor to determine if the report and request for a trace should be delayed. Even if a delay is appropriate, the report and request shall be made prior to the conclusion of the investigation (19 VAC 30-115-10).

600.10 MODIFICATION OF CHARGES FILED

Members are not authorized to recommend to the prosecutor or to any other official of the court that charges on a pending case be amended or dismissed without the authorization of a Division Supervisor or the Sheriff. Any authorized request to modify the charges or to recommend dismissal of charges shall be made to the prosecutor.

600.11 SURVEILLANCE OR UNDERCOVER EQUIPMENT

The Sheriff may provide a procedure for the authorization, distribution and use of surveillance or undercover equipment owned or issued by the Madison County Sheriff's Office.

600.12 FOLLOW-UP INVESTIGATION RESPONSIBILITIES

A follow-up investigation should include the following steps, at a minimum:

(a) Reviewing and analyzing all previous reports prepared in the preliminary phase, department records, and results from laboratory examinations, as applicable

(b) Conducting additional interviews and interrogations, if necessary

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) Seeking additional information, as appropriate (e.g., from uniformed deputies or informants)

(d) Planning, organizing, and conducting searches, if necessary

(e) Collecting physical evidence, as applicable

(f) Collecting the appropriate materials and substances from known sources when available in order to submit these items to the appropriate laboratory for a comparative analysis with the physical evidence collected

(g) Identifying and apprehending any suspect

(h) Determining if a suspect is involved in another crime

(i) Checking any suspect's criminal history

(j) Preparing the case for court presentation, if necessary

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Sexual Assault Investigations

601.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the investigation of sexual assaults. These guidelines will address some of the unique aspects of such cases and the effects that these crimes have on the victims (Va. Code § 9.1-1301).

Mandatory notification requirements are addressed in the Child Abuse and Adult Abuse policies.

601.1.1 DEFINITIONS

Definitions related to this policy include:

Sexual assault - Any crime or attempted crime of a sexual nature, including but not limited to, offenses defined in Article 7 of Chapter 4 of Title 18.2.

Sexual Assault Response Team (SART) - A multidisciplinary team generally comprised of advocates; law enforcement officers; forensic medical examiners, including sexual assault forensic examiners (SAFEs) or sexual assault nurse examiners (SANEs) if possible; forensic laboratory personnel; and prosecutors. The team is designed to coordinate a broad response to sexual assault victims.

See attachment: Madison County Sexual Assault Response Team MOU (10-30-2020).pdf

601.2 POLICY

It is the policy of the Madison County Sheriff's Office that its members, when responding to reports of sexual assaults, will strive to minimize the trauma experienced by the victims, and will aggressively investigate sexual assaults, pursue expeditious apprehension and conviction of perpetrators, and protect the safety of the victims and the community.

601.3 QUALIFIED INVESTIGATORS

Qualified investigators should be available for assignment of sexual assault investigations. These investigators should:

(a) Have specialized training in, and be familiar with, interview techniques and the medical and legal issues that are specific to sexual assault investigations.

(b) Conduct follow-up interviews and investigation.

(c) Present appropriate cases of alleged sexual assault to the prosecutor for review.

(d) Coordinate with other enforcement agencies, social service agencies and medical personnel as needed.

(e) Provide referrals to therapy services, victim advocates and support for the victim.

(f) Participate in or coordinate with the local or regional SART or other multidisciplinary investigative teams as applicable (Va. Code § 15.2-1627.4).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

601.4 REPORTING

In all reported or suspected cases of sexual assault, a report should be written and assigned for follow-up investigation. This includes incidents in which the allegations appear unfounded or unsubstantiated.

601.5 VICTIM INTERVIEWS

The primary considerations in sexual assault investigations, which begin with the initial call to the Dispatch Center, should be the health and safety of the victim, the preservation of evidence, and preliminary interviews to determine if a crime has been committed and to attempt to identify the suspect.

Whenever possible, a member of the SART should be included in the initial victim interviews.

An in-depth follow-up interview should not be conducted until after the medical and forensic examinations are completed and the personal needs of the victim have been met (e.g., change of clothes, bathing). The follow-up interview may be delayed to the following day based upon the circumstances. Whenever practicable, the follow-up interview should be conducted by a qualified investigator.

No opinion of whether the case is unfounded should be included in a report.

Victims shall not be asked or required to take a polygraph examination as a condition for proceeding with an investigation. Victims may voluntarily submit to a polygraph examination and shall be informed in writing that the results cannot be used in evidence and that their voluntary submission is not a condition for initiating or continuing the investigation (34 USC § 10451; Va. Code § 19.2-9.1).

Victims should be transported to the hospital by ambulance when appropriate based upon medical conditions or injuries. Deputies should accommodate the victim in alternative transportation for an examination if the victim does not want to be transported in a law enforcement vehicle. The deputy should also arrange for transportation of the victim after completion of the examination.

Victims should be apprised of applicable victim’s rights provisions, as outlined in the Victim and Witness Assistance Policy.

601.6 COLLECTION AND TESTING OF BIOLOGICAL EVIDENCE

Whenever possible, a SART member should be involved in the collection of forensic evidence from the victim. The SART member or deputy should not be physically present when the examination is being conducted on victims.

When the facts of the case indicate that collection of biological evidence is warranted, it should be collected regardless of how much time has elapsed since the reported assault.

If a drug-facilitated sexual assault is suspected, urine and blood samples should be collected from the victim as soon as practicable.

Subject to the requirements set forth in this policy, biological evidence from all sexual assault cases, including cases where the suspect is known by the victim, should be submitted for testing.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Victims who choose not to assist with an investigation, do not desire that the matter be investigated or wish to remain anonymous may still consent to the collection of evidence under their control. In these circumstances, the evidence should be collected and stored appropriately (Va. Code § 19.2-11.6).

601.6.1 COLLECTION AND TESTING REQUIREMENTS

Members investigating sexual assaults or handling related evidence are required to do the following:

(a) Respond promptly to a facility upon receiving notice from a health care provider that a physical evidence recovery kit has been collected (Va. Code § 19.2-11.7).

(b) Submit physical evidence recovery kits to the Virginia Department of Forensic Science (DFS) for biological testing within 60 days of receipt unless (Va. Code § 19.2-11.8):

1. The victim has chosen not to report the offense.
2. The evidence was collected by the Medical Examiner as part of a routine death investigation and the Division Supervisor and Medical Examiner agree that analysis is not necessary.
3. The offense occurred in another state.
4. Deputies, after consultation with a supervisor, determine that the evidence is not related to a criminal offense.
5. Another law enforcement agency has taken over responsibility for the investigation.
    (a) The physical evidence recovery kit should be promptly sent to the investigating agency for submission to the DFS if the investigating agency is within Virginia.

(c) Enter the identification number and any other information pertaining to a physical evidence recovery kit into the statewide electronic tracking system as required by the DFS.

Additional guidance regarding evidence retention and destruction is found in the Property and Evidence Section Policy.

601.6.2 DNA TEST RESULTS

Members investigating sexual assaults or handling related evidence should make notifications to the victim (or an appropriate family member of a victim who is a minor or who is deceased) about the submission of biological evidence for testing, the status of testing, the results of such testing, the time frame and rights related to the storage of the physical evidence recovery kit, and the kit's unique identification number and tracking information as set forth in Va. Code § 19.2-11.11.

The information required to be disclosed should be provided to the victim (or appropriate family member) as soon as reasonably practicable, unless disclosing the information would interfere with the investigation or prosecution of the case, in which case an estimated date on which the information may be available, if known, should be provided (Va. Code § 19.2-11.11).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Members are not required to provide DNA test results to a family member of a minor or deceased victim if the family member is the alleged perpetrator. In such cases, a supervisor should be consulted before any information is provided (Va. Code § 19.2-11.11).

A SART member should be consulted regarding the best way to deliver biological testing results to a victim so as to minimize victim trauma, especially in cases where there has been a significant delay in getting biological testing results (e.g., delays in testing the evidence or delayed DNA databank hits). Members should make reasonable efforts to assist the victim by providing available information on local assistance programs and organizations as provided in the Victim and Witness Assistance Policy.

Members investigating sexual assaults cases should ensure that DNA results are entered into databases when appropriate and as soon as practicable.

601.7 DISPOSITION OF CASES

If the assigned investigator has reason to believe the case is without merit, the case may be classified as unfounded only upon review and approval of the Investigation Division supervisor.

Classification of a sexual assault case as unfounded requires the Investigation Division supervisor to determine that the facts have significant irregularities with reported information and that the incident could not have happened as it was reported. When a victim has recanted his/her original statement, there must be corroborating evidence that the allegations were false or baseless (i.e., no crime occurred) before the case should be determined as unfounded.

601.8 CASE REVIEW

The Investigation Division supervisor should ensure cases are reviewed on a periodic basis, at least annually, using an identified group that is independent of the investigation process. The reviews should include an analysis of:

- Case dispositions.
- Decisions to collect biological evidence.
- Submissions of biological evidence for lab testing.

The SART and/or victim advocates should be considered for involvement in this audit. Summary reports on these reviews should be forwarded through the chain of command to the Sheriff.

601.9 RELEASING INFORMATION TO THE PUBLIC

In cases where the perpetrator is not known to the victim, and especially if there are multiple crimes where more than one appear to be related, consideration should be given to releasing information to the public whenever there is a reasonable likelihood that doing so may result in developing helpful investigative leads. The Investigation Division supervisor should weigh the risk of alerting the suspect to the investigation with the need to protect the victim and the public, and to prevent more crimes.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

601.10 TRAINING

Subject to available resources, periodic training should be provided to (Va. Code § 9.1-1301):

(a) Members who are first responders. Training should include:

1. Initial response to sexual assaults.
2. Legal issues.
3. Victim advocacy.
4. Victim’s response to trauma.

(b) Qualified investigators, who should receive advanced training on additional topics. Advanced training should include:

1. Interviewing sexual assault victims.
2. SART.
3. Medical and legal aspects of sexual assault investigations.
4. Serial crimes investigations.
5. Use of community and other federal and state investigative resources, such as the Violent Criminal Apprehension Program (ViCAP).
6. Techniques for communicating with victims to minimize trauma.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Asset Forfeiture

602.1 PURPOSE AND SCOPE

This policy describes the authority and procedure for the seizure, forfeiture and liquidation of property associated with designated offenses.

602.1.1 DEFINITIONS

Definitions related to this policy include:

Fiscal agent - The person designated by the Sheriff to be responsible for securing and maintaining seized assets and distributing any proceeds realized from any forfeiture proceedings. This includes any time the Madison County Sheriff's Office seizes property for forfeiture or when the Madison County Sheriff's Office is acting as the fiscal agent pursuant to a multi-agency agreement.

Forfeiture - The process by which legal ownership of an asset is transferred to a government or other authority.

Forfeiture reviewer - The department member assigned by the Sheriff who is responsible for reviewing all forfeiture cases and acting as the liaison between the Department and the forfeiture counsel.

Property subject to forfeiture - Property subject to forfeiture may include:

(a) Property used in connection with or derived from terrorism (Va. Code § 19.2-386.15).

(b) Vehicles used for prostitution and kidnapping related offenses (Va. Code § 19.2-386.16).

(c) Moneys and other income, including all proceeds, derived through computer crimes (Va. Code § 19.2-386.17).

(d) Property used in connection with money laundering (Va. Code § 19.2-386.19).

(e) Unlawfully sold or delivered cigarettes and counterfeit/contraband cigarettes (Va. Code § 19.2-386.20; Va. Code § 19.2-386.21).

(f) Property used in connection with or derived from illegal drug transactions (Va. Code § 19.2-386.22).

(g) Firearms carried in violation of weapons carry laws or used in a crime (Va. Code § 19.2-386.27; Va. Code § 19.2-386.28; Va. Code § 19.2-386.29).

(h) Money, gambling devices and personal property used in connection with illegal gambling (Va. Code § 19.2-386.30).

(i) Property used in connection with the exploitation, solicitation or abduction of children (Va. Code § 19.2-386.31).

(j) Money and real or personal property derived through government corruption (Va. Code § 19.2-386.33).

(k) Vehicles used in felony-level driving while intoxicated offenses (Va. Code § 19.2-386.34).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(l) Property used in connection with certain listed offenses (Va. Code § 19.2-386.35).

Seizure - The act of law enforcement officials taking property, cash or assets that have been used in connection with or acquired by specified illegal activities.

602.2 POLICY

The Madison County Sheriff's Office recognizes that appropriately applied forfeiture laws are helpful to enforce the law, deter crime and reduce the economic incentive of crime. However, the potential of revenue shall not be allowed to jeopardize the effective investigation and prosecution of criminal offenses, officer safety, the integrity of ongoing investigations or any person’s due process rights.

It is the policy of the Madison County Sheriff's Office that all members, including those assigned to internal or external law enforcement task force operations, shall comply with all state and federal laws pertaining to forfeitures.

602.3 ASSET SEIZURE

Property may be seized for forfeiture as provided in this policy.

602.3.1 PROPERTY SUBJECT TO SEIZURE

The following property may be seized upon review and approval of a supervisor and in coordination with the forfeiture reviewer:

(a) Property subject to seizure through a court order.

(b) Property that can be legally seized as evidence of a crime.

(c) Property that is not subject of a court order, but:

1. The property can be lawfully accessed by deputies.
2. There is probable cause to support a substantial connection between the property and the activity for which a statute authorizes its seizure.

Whenever practicable, obtaining a search warrant or court order for seizure prior to making a seizure is the preferred method (Va. Code § 19.2-386.2).

A large amount of money standing alone is insufficient to establish the probable cause required to make a seizure.

602.3.2 PROPERTY NOT SUBJECT TO SEIZURE

The following property should not be seized for forfeiture:

(a) Cash and property that does not meet the forfeiture counsel’s current minimum forfeiture thresholds.

(b) Property when the deputy suspects the owner was not a consenting party or privy to the conduct giving rise to forfeiture ("innocent owner") (Va. Code § 19.2-386.8).

(c) Real property absent a court order.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

602.3.3 REQUESTS TO RELINQUISH PROPERTY RIGHTS

Deputies shall not request or otherwise suggest that a person who is asserting an ownership or other right to property seized by the department waive that interest prior to the filing of an information related to the property (Va. Code § 19.2-386.2).

602.4 PROCESSING SEIZED PROPERTY FOR FORFEITURE PROCEEDINGS

When property or cash subject to this policy is seized, the deputy making the seizure should ensure compliance with the following:

(a) Complete the applicable seizure forms and present the appropriate copy to the person from whom the property is seized. If cash or property is seized from more than one person, a separate copy must be provided to each person, specifying the items seized. When property is seized and no one claims an interest in the property, the deputy must leave the copy in the place where the property was found, if it is reasonable to do so (Va. Code § 19.2-386.2).

(b) Complete and submit a report and original seizure forms within 24 hours of the seizure, if practicable.

(c) Forward the original seizure forms and related reports to the forfeiture reviewer within one day of seizure.

The deputy will book seized property as evidence with the notation in the comment section of the property form, "Seized Subject to Forfeiture." Property seized subject to forfeiture should be booked on a separate property form. No other evidence from the case should be booked on this form.

Photographs should be taken of items seized, particularly cash, jewelry and other valuable items.

Deputies who suspect property may be subject to seizure but are not able to seize the property (e.g., the property is located elsewhere; the whereabouts of the property is unknown; it is real estate, bank accounts, non-tangible assets) should document and forward the information in the appropriate report to the forfeiture reviewer.

602.5 MAINTAINING SEIZED PROPERTY

The Property and Evidence Section supervisor is responsible for ensuring compliance with the following:

(a) All property received for forfeiture is reasonably secured and properly stored to prevent waste and preserve its condition (Va. Code § 19.2-386.4).

(b) All property received for forfeiture is checked to determine whether the property has been stolen.

(c) All property received for forfeiture is retained in the same manner as evidence until forfeiture is finalized or the property is returned to the claimant or the person with an ownership interest.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Property received for forfeiture is not used unless the forfeiture action has been completed.

(e) Forfeitable property is retained until such time as its use as evidence is no longer required.

602.6 FORFEITURE REVIEWER

The Sheriff will appoint a forfeiture reviewer. Prior to assuming duties, or as soon as practicable thereafter, the forfeiture reviewer should attend a course approved by the Department on asset forfeiture.

The responsibilities of the forfeiture reviewer include:

(a) Remaining familiar with state and federal forfeiture laws, particularly the Va. Code § 19.2-386.1 et seq. and the forfeiture policies of forfeiture counsel.

(b) Serving as the liaison between the Department and the forfeiture counsel and ensuring prompt legal review of all seizures.

1. If property was seized before an information was filed, notification to the forfeiture attorney should occur as soon as practicable (Va. Code § 19.2-386.3).

(c) Making reasonable efforts to obtain annual training that includes best practices in pursuing, seizing, and tracking forfeitures.

(d) Reviewing each seizure-related case and deciding whether the seizure is more appropriately made under state or federal seizure laws. The forfeiture reviewer should contact federal authorities when appropriate.

(e) Ensuring that responsibilities, including the designation of a fiscal agent, are clearly established whenever multiple agencies are cooperating in a forfeiture case.

(f) Ensuring that seizure forms are available and appropriate for department use. These should include notice forms, a receipt form, and a checklist that provides relevant guidance to deputies. The forms should be available in languages appropriate for the region and should contain spaces for:

1. Names and contact information for all relevant persons and law enforcement officers involved.

2. Information as to how ownership or other property interests may have been determined (e.g., verbal claims of ownership, titles, public records).

3. A space for the signature of the person from whom cash or property is being seized.

4. A tear-off portion or copy, which should be given to the person from whom cash or property is being seized, that includes the legal authority for the seizure, information regarding the process to contest the seizure, and a detailed description of the items seized.

(g) Ensuring that deputies who may be involved in asset forfeiture receive training in the proper use of the seizure forms and the forfeiture process. The training should be developed in consultation with the appropriate legal counsel and may be accomplished

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

through traditional classroom education, electronic media, Daily Training Bulletins (DTBs), or General Orders. The training should cover this policy and address any relevant statutory changes and court decisions.

(h) Reviewing each asset forfeiture case to ensure that:

1. Written documentation of the seizure and the items seized is in the case file.
2. Independent legal review of the circumstances and propriety of the seizure is made in a timely manner.
3. Notice of seizure has been given in a timely manner to those who hold an interest in the seized property.
4. Property is promptly released to those entitled to its return.
5. All changes to forfeiture status are forwarded to any supervisor who initiates a forfeiture case.
6. Any cash received is deposited with the fiscal agent.
   (a) The cash shall be held in an interest-bearing account (Va. Code § 19.2-386.4).
7. Assistance with the resolution of ownership claims and the release of property to those entitled is provided.
8. Current minimum forfeiture thresholds are communicated appropriately to deputies.
9. This policy and any related policies are periodically reviewed and updated to reflect current federal and state statutes and case law.

(i) Ensuring that a written plan is available that enables the Sheriff to address any extended absence of the forfeiture reviewer, thereby ensuring that contact information for other law enforcement personnel and attorneys who may assist in these matters is available.

(j) Ensuring that the Department disposes of property as provided by law following any forfeiture.

(k) Ensuring that the process of selling or adding forfeited property to department inventory is in accordance with all applicable laws and consistent with the use and disposition of similar property.

(l) Upon completion of any forfeiture process, ensuring that no property is retained by the Madison County Sheriff's Office unless the Sheriff authorizes in writing the retention of the property for official use.

(m) Forwarding a report regarding seized property subject to forfeiture, its release, or other final disposition of the property with the Department of Criminal Justice Services (DCJS) as may be required (Va. Code § 19.2-386.4; 6 VAC 20-150-30).

(n) After consultation with the Sheriff, filing a DCJS Form 999 with the DCJS after a court has ordered assets to be forfeited and when the Madison County Sheriff's Office is the designated seizing agency, as well as any other notifications that may be required by law (6 VAC 20-150-40; Va. Code § 19.2-386.14).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(o) Ensuring that an annual financial statement of receipts and expenditures is filed with the DCJS as may be required (6 VAC 20-150-40).

Forfeiture proceeds should be maintained in a separate fund or account subject to appropriate accounting control, with regular reviews or audits of all deposits and expenditures.

Forfeiture reporting and expenditures should be completed in the manner prescribed by the law and County financial directives.

602.7 DISPOSITION OF FORFEITED PROPERTY

All proceeds from a forfeiture will be used for law enforcement purposes only and will not be used to supplant existing funds from any source (6 VAC 20-150-80).

No member of this department may use property that has been seized for forfeiture until the forfeiture action has been completed and the Sheriff has given written authorization to retain the property for official use. No department member involved in the decision to seize property should be involved in any decision regarding the disposition of the property.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Informants

603.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the use of informants.

603.1.1 DEFINITIONS

Definitions related to this policy include:

Informant - A person who covertly interacts with other individuals or suspects at the direction or request of, or by agreement with, the Madison County Sheriff's Office for law enforcement purposes. This also includes a person agreeing to supply information to the Madison County Sheriff's Office for a benefit (e.g., a quid pro quo in the form of a reduced criminal penalty, money).

603.2 POLICY

The Madison County Sheriff's Office recognizes the value of informants to law enforcement efforts and will strive to protect the integrity of the informant process. It is the policy of this department that all funds related to informant payments will be routinely audited and that payments to informants will be made according to the criteria outlined in this policy.

603.3 USE OF INFORMANTS

603.3.1 INITIAL APPROVAL

Before using an individual as an informant, a deputy must receive approval from his/her supervisor. The deputy shall compile sufficient information through a background investigation and experience with the informant in order to determine the suitability of the individual, including age, maturity and risk of physical harm, as well as any indicators of his/her reliability and credibility.

Members of this department should not guarantee absolute safety or confidentiality to an informant.

603.3.2 JUVENILE INFORMANTS

The use of informants under the age of 13 is prohibited.

In all cases, a juvenile 13 years of age or older may only be used as an informant with the written consent of each of the following:

(a) The juvenile’s parents or legal guardians

(b) The juvenile’s attorney, if any

(c) The court in which the juvenile’s case is being handled, if applicable

(d) The Sheriff or the authorized designee

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

603.3.3 INFORMANT AGREEMENTS
All informants are required to sign and abide by the provisions of the designated department informant agreement. The deputy using the informant shall discuss each of the provisions of the agreement with the informant.

Details of the agreement are to be approved in writing by a supervisor before being finalized with the informant.

603.4 INFORMANT INTEGRITY

To maintain the integrity of the informant process, the following must be adhered to:

(a) The identity of an informant acting in a confidential capacity shall not be withheld from the Sheriff, Division Supervisor, Investigations supervisor or their authorized designees.

1. Identities of informants acting in a confidential capacity shall otherwise be kept confidential.

(b) Criminal activity by informants shall not be condoned.

(c) Informants shall be told they are not acting as sheriff's deputies, employees or agents of the Madison County Sheriff's Office, and that they shall not represent themselves as such.

(d) The relationship between department members and informants shall always be ethical and professional.

1. Members shall not become intimately involved with an informant.

2. Social contact shall be avoided unless it is necessary to conduct an official investigation, and only with prior approval of the Investigations supervisor.

3. Members shall neither solicit nor accept gratuities or engage in any private business transaction with an informant.

(e) Deputies shall not meet with informants in a private place unless accompanied by at least one additional deputy or with prior approval of the Investigations supervisor.

1. Deputies may meet informants alone in an occupied public place, such as a restaurant.

(f) When contacting informants for the purpose of making payments, deputies shall arrange for the presence of another deputy.

(g) In all instances when department funds are paid to informants, a voucher shall be completed in advance, itemizing the expenses.

(h) Since the decision rests with the appropriate prosecutor, deputies shall not promise that the informant will receive any form of leniency or immunity from criminal prosecution.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

603.4.1 UNSUITABLE INFORMANTS

The suitability of any informant should be considered before engaging him/her in any way in a covert or other investigative process. Members who become aware that an informant may be unsuitable will notify the supervisor, who will initiate a review to determine suitability. Until a determination has been made by a supervisor, the informant should not be used by any member. The supervisor shall determine whether the informant should be used by the Department and, if so, what conditions will be placed on his/her participation or any information the informant provides. The supervisor shall document the decision and conditions in file notes and mark the file “unsuitable” when appropriate.

Considerations for determining whether an informant is unsuitable include, but are not limited to, the following:

(a) The informant has provided untruthful or unreliable information in the past.

(b) The informant behaves in a way that may endanger the safety of a deputy.

(c) The informant reveals to suspects the identity of a deputy or the existence of an investigation.

(d) The informant appears to be using his/her affiliation with this department to further criminal objectives.

(e) The informant creates officer-safety issues by providing information to multiple law enforcement agencies simultaneously, without prior notification and approval of each agency.

(f) The informant engages in any other behavior that could jeopardize the safety of deputies or the integrity of a criminal investigation.

(g) The informant commits criminal acts subsequent to entering into an informant agreement.

603.5 INFORMANT FILES

Informant files shall be utilized as a source of background information about the informant, to enable review and evaluation of information provided by the informant, and to minimize incidents that could be used to question the integrity of department members or the reliability of the informant.

Informant files shall be maintained in a secure area within the Investigations. The Investigations supervisor or the authorized designee shall be responsible for maintaining informant files. Access to the informant files shall be restricted to the Sheriff, Division Supervisor, Investigations supervisor or their authorized designees.

The Investigation Division Supervisor should arrange for an audit using a representative sample of randomly selected informant files on a periodic basis, but no less than one time per year. If the Investigations supervisor is replaced, the files will be audited before the new supervisor takes over management of the files. The purpose of the audit is to ensure compliance with file content

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

and updating provisions of this policy. The audit should be conducted by a supervisor who does not have normal access to the informant files.

603.5.1 FILE SYSTEM PROCEDURE

A separate file shall be maintained on each informant and shall be coded with an assigned informant control number. An informant history that includes the following information shall be prepared for each file:

(a) Name and aliases

(b) Date of birth

(c) Physical description: sex, race, height, weight, hair color, eye color, scars, tattoos or other distinguishing features

(d) Photograph

(e) Current home address and telephone numbers

(f) Current employers, positions, addresses and telephone numbers

(g) Vehicles owned and registration information

(h) Places frequented

(i) Briefs of information provided by the informant and his/her subsequent reliability

1. If an informant is determined to be unsuitable, the informant's file is to be marked "unsuitable" and notations included detailing the issues that caused this classification.

(j) Name of the deputy initiating use of the informant

(k) Signed informant agreement

(l) Update on active or inactive status of informant

603.6 INFORMANT PAYMENTS

No informant will be told in advance or given an exact amount or percentage for his/her service. The amount of funds to be paid to any informant will be evaluated against the following criteria:

- The significance, value or effect on crime
- The value of assets seized
- The quantity of the drugs or other contraband seized
- The informant’s previous criminal activity
- The level of risk taken by the informant

The Investigations supervisor will discuss the above factors with the Patrol Division Supervisor and recommend the type and level of payment, subject to approval by the Sheriff.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

603.6.1 PAYMENT PROCESS

Approved payments to an informant should be in cash using the following process:

(a) Payments of $500 and under may be paid in cash from a Investigations buy/expense fund.

1. The Investigations supervisor shall sign the voucher for cash payouts from the buy/expense fund.

(b) Payments exceeding $500 shall be made by issuance of a check, payable to the deputy who will be delivering the payment.

1. The check shall list the case numbers related to and supporting the payment.
2. A written statement of the informant's involvement in the case shall be placed in the informant's file.
3. The statement shall be signed by the informant verifying the statement as a true summary of his/her actions in the case.
4. Authorization signatures from the Sheriff and the County Administrator are required for disbursement of the funds.

(c) To complete the payment process for any amount, the deputy delivering the payment shall complete a cash transfer form.

1. The cash transfer form shall include:
   (a) Date.
   (b) Payment amount.
   (c) Madison County Sheriff's Office case number.
   (d) A statement that the informant is receiving funds in payment for information voluntarily rendered.
2. The cash transfer form shall be signed by the informant.
3. The cash transfer form will be kept in the informant’s file.

603.6.2 REPORTING OF PAYMENTS

Each informant receiving a cash payment shall be advised of his/her responsibility to report the cash to the Internal Revenue Service (IRS) as income. If funds distributed exceed $600 in any reporting year, the informant should be provided IRS Form 1099 (26 CFR 1.6041-1). If such documentation or reporting may reveal the identity of the informant and by doing so jeopardize any investigation, the safety of deputies or the safety of the informant (26 CFR 1.6041-3), then IRS Form 1099 should not be issued.

In such cases, the informant shall be provided a letter identifying the amount he/she must report on a tax return as “other income” and shall be required to provide a signed acknowledgement

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

of receipt of the letter. The completed acknowledgement form and a copy of the letter shall be retained in the informant's file.

603.6.3 AUDIT OF PAYMENTS

The Investigations supervisor or the authorized designee shall be responsible for compliance with any audit requirements associated with grant provisions and applicable state and federal law.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Eyewitness Identification

604.1 PURPOSE AND SCOPE

This policy sets forth guidelines to be used when members of this department employ eyewitness identification techniques (Va. Code § 19.2-390.02).

604.1.1 DEFINITIONS

Definitions related to this policy include:

Eyewitness identification process - Any field identification, live lineup, or photographic identification.

Field identification - A live presentation of a single individual to a witness following the commission of a criminal offense for the purpose of identifying or eliminating the person as the suspect.

Live lineup - A live presentation of individuals to a witness for the purpose of identifying or eliminating an individual as the suspect.

Photographic lineup - Presentation of photographs to a witness for the purpose of identifying or eliminating an individual as the suspect.

604.2 POLICY

The Madison County Sheriff's Office will strive to use eyewitness identification techniques, when appropriate, to enhance the investigative process and will emphasize identifying persons responsible for crime and exonerating the innocent. Use of these procedures should maximize the reliability of identifications, minimize unjust accusations of innocent persons and establish evidence that is reliable and conforms to established legal procedure.

Madison County Sheriff's Office Law Enforcement Procedures Manual: 604.1 Legal Review of Eyewitness Identification Procedures

604.3 INTERPRETIVE SERVICES

Members should make a reasonable effort to arrange for an interpreter before proceeding with eyewitness identification if communication with a witness is impeded due to language or hearing barriers.

Before the interpreter is permitted to discuss any matter with the witness, the investigating member should explain the identification process to the interpreter. Once it is determined that the interpreter comprehends the process and can explain it to the witness, the eyewitness identification may proceed as provided for within this policy.

604.4 EYEWITNESS IDENTIFICATION FORM

The Investigation Division supervisor shall be responsible for the development and maintenance of an eyewitness identification process for use by members when they are conducting eyewitness identifications.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

The process should include appropriate forms or reports that provide:

(a) The date, time and location of the eyewitness identification procedure.

(b) The name and identifying information of the witness.

(c) The name of the person administering the identification procedure.

(d) If applicable, the names of all individuals present during the identification procedure.

(e) An instruction to the witness that it is as important to exclude innocent persons as it is to identify a perpetrator.

(f) An instruction to the witness that the perpetrator may or may not be among those presented and that the witness is not obligated to make an identification.

(g) If the identification process is a photographic or live lineup, an instruction to the witness that the perpetrator may not appear exactly as he/she did on the date of the incident.

(h) An instruction to the witness that the investigation will continue regardless of whether an identification is made by the witness.

(i) A signature line where the witness acknowledges that he/she understands the identification procedures and instructions.

(j) A statement from the witness in the witness's own words describing how certain he/she is of the identification or non-identification. This statement should be taken at the time of the identification procedure.

The process and related forms should be reviewed at least annually and modified when necessary.

See attachment: 604 Eyewitness Lineup Instruction Form.pdf

See attachment: 604 Eyewitness Sequential Photo Lineup Instruction Form.pdf

See attachment: 604 Eyewitness Show-up Instruction Form.pdf

See attachment: 604 Lineup Results Form.pdf

See attachment: 604 Lineup Case Information Sheet.pdf

604.4.1 CONFERENCE WITH PROSECUTOR

The Investigation Division should confer with the Office of the Commonwealth's Attorney and consult the Virginia Model Policy on Eyewitness Investigation issued by the Virginia Department of Criminal Justice Services when developing, reviewing and revising the witness identification process in order to ensure that the procedures established are compatible and consistent with the Virginia Department of Criminal Justice Services Model Policy on Eyewitness Identification (March 19, 2014), as appropriate.

604.5 EYEWITNESS IDENTIFICATION

Members are cautioned not to, in any way, influence a witness as to whether any subject or photo presented in a lineup is in any way connected to the case. Members should avoid mentioning that:

- The individual was apprehended near the crime scene.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

- The evidence points to the individual as the suspect.
- Other witnesses have identified or failed to identify the individual as the suspect.

In order to avoid undue influence, witnesses should view suspects or a lineup individually and outside the presence of other witnesses. Witnesses should be instructed to avoid discussing details of the incident or of the identification process with other witnesses.

Whenever feasible, the eyewitness identification procedure should be audio and/or video recorded and the recording should be retained according to current evidence procedures.

604.6 PHOTOGRAPHIC LINEUP AND IN-PERSON LINEUP CONSIDERATIONS

When practicable, the member presenting the lineup should not be involved in the investigation of the case or know the identity of the suspect. In no case should the member presenting a lineup to a witness know which photograph or person in the lineup is being viewed by the witness. Techniques to achieve this include randomly numbering photographs, shuffling folders, or using a computer program to order the persons in the lineup.

Individuals in the lineup should reasonably match the description of the perpetrator provided by the witness and should bear similar characteristics to avoid causing any person to unreasonably stand out. In cases involving multiple suspects, a separate lineup should be conducted for each suspect. The suspects should be placed in a different order within each lineup.

The member presenting the lineup should do so sequentially (i.e., show the witness one person at a time) and not simultaneously. The witness should view all persons in the lineup.

A live lineup should only be used before criminal proceedings have been initiated against the suspect. If there is any question as to whether any criminal proceedings have begun, the investigating member should contact the appropriate prosecuting attorney before proceeding.

Madison County Sheriff's Office Law Enforcement Procedures Manual: 605.1 Live/Photo Lineup Procedures

Madison County Sheriff's Office Law Enforcement Procedures Manual: 605.2 Folder Shuffle Method

604.7 FIELD IDENTIFICATION CONSIDERATIONS

Field identifications, also known as field elimination show-ups or one-on-one identifications, may be helpful in certain cases, where exigent circumstances make it impracticable to conduct a photo or live lineup identification. A field elimination show-up or one-on-one identification should not be used when independent probable cause exists to arrest a suspect. In such cases, a live or photo lineup is the preferred course of action if eyewitness identification is contemplated.

Madison County Sheriff's Office Law Enforcement Procedures Manual: 606.1 Field Identification Procedures

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Eyewitness Identification

604.8 DOCUMENTATION

A thorough description of the eyewitness process and the result of any eyewitness identification should be documented in the case report.

If a photographic lineup is utilized, a copy of the photographic lineup presented to the witness should be included in the case report. In addition, the order in which the photographs were presented to the witness should be documented in the case report.

Department personnel shall report any known errors, flaws or non-conformance with established procedures in the conduct of a suspect lineup that they may observe or become aware of to their supervisor in order that corrective actions may be taken and safeguards established to protect the innocent.

604.9 TRAINING

The Madison County Sheriff's Office should establish minimum standards of training in eyewitness identification procedures for members. The purpose of this training is to:

(a) Ensure uniformity and consistency in eyewitness identification.

(b) Establish and maintain a high level of member competence in eyewitness identification and to prepare members for this important aspect of criminal investigation.

The Training Supervisor shall ensure that members receive initial and periodic training in eyewitness identification and on this policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Brady Information

605.1 PURPOSE AND SCOPE

This policy establishes guidelines for identifying and releasing potentially exculpatory or impeachment information (so-called "*Brady* information") to a prosecuting attorney.

605.1.1 DEFINITIONS

Definitions related to this policy include:

***Brady* information** - Information known or possessed by the Madison County Sheriff's Office that is both favorable and material to the current prosecution or defense of a criminal defendant.

605.2 POLICY

The Madison County Sheriff's Office will conduct fair and impartial criminal investigations and will provide the prosecution with both incriminating and exculpatory evidence, as well as information that may adversely affect the credibility of a witness. In addition to reporting all evidence of guilt, the Madison County Sheriff's Office will assist the prosecution by complying with its obligation to disclose information that is both favorable and material to the defense. The Department will identify and disclose to the prosecution potentially exculpatory information, as provided in this policy.

605.3 DISCLOSURE OF INVESTIGATIVE INFORMATION

Deputies must include in their investigative reports adequate investigative information and reference to all material evidence and facts that are reasonably believed to be either incriminating or exculpatory to any individual in the case. If a deputy learns of potentially incriminating or exculpatory information any time after submission of a case, the deputy or the handling investigator must prepare and submit a supplemental report documenting such information as soon as practicable. Supplemental reports shall be promptly processed and transmitted to the prosecutor's office.

If information is believed to be privileged or confidential (e.g., informant, attorney-client information, attorney work product), the deputy should discuss the matter with a supervisor and/or prosecutor to determine the appropriate manner in which to proceed.

Evidence or facts are considered material if there is a reasonable probability that they would affect the outcome of a criminal proceeding or trial. Determining whether evidence or facts are material often requires legal or even judicial review. If a deputy is unsure, the deputy should address the issue with a supervisor.

Supervisors who are uncertain about whether evidence or facts are material should address the issue in a written memo to an appropriate prosecutor. A copy of the memo should be retained in the department case file.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

605.4 BRADY PROCESS

The Sheriff shall select a member of the Department to coordinate requests for *Brady* information. This person shall be directly responsible to the Administration Division Supervisor or the authorized designee.

The responsibilities of the coordinator include but are not limited to:

(a) Working with the appropriate prosecutors' offices and the County Attorney's office to establish systems and processes to determine what constitutes *Brady* information and the method for notification and disclosure.

(b) Maintaining a current list of members who have *Brady* information in their files or backgrounds.

1. Updating this list whenever potential *Brady* information concerning any department member becomes known to the Department or is placed into a personnel or internal affairs file.

605.4.1 RECORDS RELATED TO PERSONNEL COMPLAINTS

The member selected by the Sheriff to coordinate requests for *Brady* information is also responsible for establishing a system to comply with the requirements of Va. Code § 19.2-201 regarding personnel complaints against a deputy who is a witness in a criminal matter or under criminal investigation related to the performance of that deputy's duties (Va. Code § 19.2-201).

Any dissemination of records related to personnel complaints shall be in compliance with state and federal law, as well as this policy and the Personnel Records and Personnel Complaints policies. Protective orders and/or redactions should be sought as appropriate.

605.5 DISCLOSURE OF REQUESTED INFORMATION

If *Brady* information is located, the following procedure shall apply:

(a) In the event that a motion has not already been filed by the criminal defendant or other party, the Commonwealth's attorney and the department member whose file is related to the motion shall be notified of the potential presence of *Brady* information.

(b) The Commonwealth's attorney should be requested to file a motion in order to initiate an in-camera review by the court.

1. If no motion is filed, the Records Manager should work with the Commonwealth's attorney to determine whether the records should be disclosed to the prosecutor.

(c) The Records Manager shall accompany all relevant personnel files during any in-camera inspection and address any issues or questions raised by the court in determining whether any information contained in the files is both material and favorable to the criminal defendant.

(d) If the court determines that there is relevant *Brady* information contained in the files, only that information ordered released will be copied and released to the parties filing the motion.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1. Prior to the release of any information pursuant to this process, a protective order should be requested from the court limiting the use of such information to the involved case and requiring the return of all copies upon completion of the case.

(e) If a court has determined that relevant *Brady* information is contained in a member's file in any case, the Commonwealth's attorney should be notified of that fact in all future cases involving that member.

605.6 INVESTIGATING BRADY ISSUES

If the Department receives information from any source that a member may have issues of credibility or dishonesty or has been engaged in an act of moral turpitude or criminal conduct, the information shall be investigated and processed in accordance with the Personnel Complaints Policy.

605.7 SUBPOENA PROCESSING

The individual processing subpoenas (or the supervisor of the subpoenaed member) shall check the subpoenaed member's name against the current list of those who are known to have *Brady* information in their files or background, and shall alert the coordinator if a person on the list is subpoenaed.

605.8 TRAINING

Department personnel should receive periodic training on the requirements of this policy.

See attachment: 605 IACP Brady-Giglio Training Outline.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Unmanned Aerial System

606.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the use of an unmanned aerial system (UAS) and for the storage, retrieval and dissemination of images and data captured by the UAS.

606.1.1 DEFINITIONS

Definitions related to this policy include:

Unmanned aerial system (UAS) - An unmanned aircraft of any type that is capable of sustaining directed flight, whether preprogrammed or remotely controlled (commonly referred to as an unmanned aircraft vehicle (UAV)), and all of the supporting or attached systems designed for gathering information through imaging, recording or any other means.

606.2 POLICY

A UAS may be utilized to enhance the department's mission of protecting lives and property when other means and resources are not available or are less effective. Any use of a UAS will be in strict accordance with Virginia law, constitutional and privacy rights and Federal Aviation Administration (FAA) regulations.

606.3 PRIVACY

The use of the UAS potentially involves privacy considerations. Absent a legitimate public safety mission, training, or for demonstration purposes, operators and observers shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure). Operators and observers shall take reasonable precautions to avoid inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy. Reasonable precautions can include, for example, deactivating or turning imaging devices away from such areas or persons during UAS operations.

606.4 PROGRAM COORDINATOR

The Sheriff will appoint a program coordinator who will be responsible for the management of the UAS program. The program coordinator will ensure that policies and procedures conform to current laws, regulations, and best practices and will have the following additional responsibilities:

- Coordinating the FAA Certificate of Waiver or Authorization (COA) application process and ensuring that the COA is current, and/or coordinating compliance with FAA Part 107 Remote Pilot Certificate, as appropriate for department operations.
- Ensuring that all authorized operators and required observers have completed all required FAA and department-approved training in the operation, applicable laws, policies, and procedures regarding use of the UAS.
- Developing uniform protocols for submission and evaluation of requests to deploy a UAS, including urgent requests made during ongoing or emerging incidents. Deployment of a UAS shall require written authorization of the Sheriff or the authorized designee, depending on the type of mission.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

- Coordinating the completion of the FAA Emergency Operation Request Form in emergency situations, as applicable (e.g., natural disasters, search and rescue, emergency situations to safeguard human life).
- Developing protocols for conducting criminal investigations involving a UAS, including documentation of time spent monitoring a subject.
- Implementing a system for public notification of UAS deployment.
- Developing operational protocols governing the deployment and operation of a UAS including but not limited to safety oversight, use of visual observers, establishment of lost link procedures, and secure communication with air traffic control facilities.
- Developing a protocol for fully documenting all missions. Documentation shall include a flight log which captures flight time, duration, date, supervisory authorization, and reason for flight.
- Developing a UAS inspection, maintenance, and record-keeping protocol to ensure continuing airworthiness of a UAS, up to and including its overhaul or life limits.
- Developing protocols to ensure that all data intended to be used as evidence are accessed, maintained, stored, and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, authenticity certificates, and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.
- Developing protocols that ensure retention and purge periods are maintained in accordance with established records retention schedules.
- Facilitating law enforcement access to images and data captured by the UAS.
- Recommending program enhancements, particularly regarding safety and information security.
- Ensuring that established protocols are followed by monitoring and providing periodic reports on the program to the Sheriff.
- Maintaining documentation on UAS use, including a flight log that captures flight time, duration, date, supervisory authorization, and reason for flight.
- Maintaining familiarity with FAA regulatory standards, state laws and regulations, and local ordinances regarding the operations of a UAS.

606.5 USE OF UAS

Only authorized operators who have completed the required training shall be permitted to operate the UAS.

Use of vision enhancement technology (e.g., thermal and other imaging equipment not generally available to the public) is permissible in viewing areas only where there is no protectable privacy interest or when in compliance with a search warrant or court order. In all other instances, legal counsel should be consulted.

UAS operations should only be conducted consistent with FAA regulations.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

UAS shall only be used (Va. Code § 19.2-60.1):

(a) Pursuant to a valid search, administrative, or inspection warrant.

(b) Without a warrant:

1. When an Amber Alert™, Senior Alert, or Blue Alert has been activated.
2. When necessary to alleviate an immediate danger to any person.
3. To support purposes other than law enforcement, such as assessing damage, traffic conditions, floods, or wildfires.
4. As part of a training exercise related to authorized uses.
5. When consent is given by a person with legal authority to consent to the warrantless search.
6. Following an accident where a report is required by Va. Code § 46.2-373 in order to survey the scene for a crash reconstruction or to record the scene by photographs or video.
7. To aid in planning for the execution of an existing arrest warrant or bench warrant for a felony offense at the subject's primary residence.
8. To locate a person sought for arrest when that person has fled and a law enforcement officer is in hot pursuit.

606.6 PROHIBITED USE

The UAS video surveillance equipment shall not be used:

- To conduct random surveillance activities.
- To target a person based solely on actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability.
- To harass, intimidate, or discriminate against any individual or group.
- To conduct personal business of any type.

The UAS shall not be weaponized (Va. Code § 19.2-60.1).

606.7 RETENTION OF UAS DATA

Data collected by the UAS shall be retained as provided in the established records retention schedule.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Warrant Service

607.1 PURPOSE AND SCOPE

This policy establishes guidelines for the planning and serving of arrest and search warrants by members of this department. It is understood that this policy cannot address every variable or circumstance that can arise in the service of a search or arrest warrant, as these tasks can involve rapidly evolving and unique circumstances.

This policy is intended to be used in conjunction with the Operations Planning and Deconfliction Policy, which has additional guidance on planning and serving high-risk warrants.

This policy is not intended to address the service of search warrants on locations or property already secured or routine field warrant arrests by patrol officers.

607.2 POLICY

It is the policy of the Madison County Sheriff's Office to balance the safety needs of the public, the safety of department members, privacy interests and other relevant factors when making decisions related to the service of search and arrest warrants.

607.3 OPERATIONS DIRECTOR

The operations director (see the Operations Planning and Deconfliction Policy) shall review all risk assessment forms with the involved supervisor to determine the risk level of the warrant service.

The operations director will also have the responsibility to coordinate service of those warrants that are categorized as high risk. Deconfliction, risk assessment, operational planning, briefing and debriefing should follow guidelines in the Operations Planning and Deconfliction Policy.

607.4 SEARCH WARRANTS

Deputies should receive authorization from a supervisor before preparing a search warrant affidavit. Once authorization is received, the deputy will prepare the affidavit and search warrant, consulting with the applicable prosecuting attorney as needed. He/she will also complete the risk assessment form and submit it, along with the warrant affidavit, to the appropriate supervisor and the operations director for review and classification of risk (see the Operations Planning and Deconfliction Policy).

607.5 ARREST WARRANTS

If a deputy reasonably believes that serving an arrest warrant may pose a higher risk than commonly faced on a daily basis, the deputy should complete the threat assessment form and submit it to the appropriate supervisor and the operations director for review and classification of risk (see the Operations Planning and Deconfliction Policy).

If the warrant is classified as high risk, service will be coordinated by the operations director. If the warrant is not classified as high risk, the supervisor should weigh the risk of entry into a residence to make an arrest against other alternatives, such as arresting the person outside the residence where circumstances may pose a lower risk.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

607.6 WARRANT PREPARATION

A deputy who prepares a warrant should ensure the documentation in support of the warrant contains as applicable:

(a) Probable cause to support the search or arrest, including relevant dates and times to demonstrate timeliness and facts to support any request for nighttime warrant execution (Va. Code § 19.2-56).

(b) A clear explanation of the affiant's training, experience, and relevant education.

(c) Adequately supported opinions, when relevant, that are not left to unsubstantiated conclusions.

(d) A nexus between the place to be searched and the persons or items central to the investigation. The facts supporting this nexus should be clear and current. For example, the affidavit shall explain why there is probable cause to believe that a particular person is currently residing at a particular location or that the items sought are present at a particular location.

(e) Full disclosure of known or suspected residents at the involved location and any indication of separate living spaces at the involved location. For example, it should be disclosed that several people may be renting bedrooms at a single location, even if the exact location of the rooms is not known.

(f) A specific description of the location to be searched, including photographs of the location, if reasonably available.

(g) A sufficient description of the items to be seized.

(h) Full disclosure of any known exculpatory information relevant to the warrant application (refer to the *Brady* Information Policy).

607.7 HIGH-RISK WARRANT SERVICE

The operations director or the authorized designee shall coordinate the service of warrants that are categorized as high risk and shall have sole authority in determining the manner in which the warrant will be served, including the number of deputies deployed.

The member responsible for directing the service should ensure the following as applicable:

(a) When practicable and when doing so does not cause unreasonable risk, video or photographic documentation is made of the condition of the location prior to execution of a search warrant. The images should include the surrounding area and persons present.

(b) The warrant service is audio- and video-recorded when practicable and reasonable to do so.

(c) Evidence is handled and collected only by those members who are designated to do so. All other members involved in the service of the warrant should alert one of the designated members to the presence of potential evidence and not touch or disturb the items.

(d) Reasonable efforts are made during the search to maintain or restore the condition of the location.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(e) Persons who are detained as part of the warrant service are handled appropriately under the circumstances.

(f) Reasonable care provisions are made for children and dependent adults (see the Child and Dependent Adult Safety Policy).

(g) A list is made of all items seized and a copy provided to the person in charge of the premises if present or otherwise left in a conspicuous place.

(h) A copy of the search warrant is left at the location.

(i) The condition of the property is documented with video recording or photographs after the search.

See attachment: Threat Assessment Matrix.pdf

607.8 DETENTIONS DURING WARRANT SERVICE

Deputies must be sensitive to the safety risks of all persons involved with the service of a warrant. Depending on circumstances and facts present, it may be appropriate to control movements of any or all persons present at a warrant service, including those who may not be the subject of a warrant or suspected in the case. However, deputies must be mindful that only reasonable force may be used and weapons should be displayed no longer than the deputy reasonably believes is necessary (see the Use of Force Policy).

As soon as it can be determined that an individual is not subject to the scope of a warrant and that no further reasonable suspicion or safety concerns exist to justify further detention, the person should be promptly released.

Deputies should, when and to the extent reasonable, accommodate the privacy and personal needs of people who have been detained.

607.9 ACTIONS AFTER WARRANT SERVICE

The supervisor shall ensure that all affidavits, warrants, receipts and returns, regardless of any associated cases, are filed with the issuing judge or magistrate as soon as reasonably possible, but in any event no later than any date specified on the warrant.

607.10 OUTSIDE AGENCIES AND CROSS-JURISDICTIONAL WARRANTS

The operations director will ensure that cooperative efforts with other agencies in the service of warrants conform to existing mutual aid agreements or other memorandums of understanding and will work cooperatively to mitigate risks including, but not limited to, the following:

- Identity of team members
- Roles and responsibilities
- Familiarity with equipment
- Rules of engagement
- Asset forfeiture procedures

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Any outside agency requesting assistance in the service of a warrant within this jurisdiction should be referred to the operations director. The director should review and confirm the warrant, including the warrant location, and should discuss the service with the appropriate supervisor from the other agency. The director should ensure that members of the Madison County Sheriff's Office are utilized appropriately. Any concerns regarding the requested use of Madison County Sheriff's Office members should be brought to the attention of the Sheriff or the authorized designee. The actual service of the warrant will remain the responsibility of the agency requesting assistance.

If the operations director is unavailable, the Shift Supervisor should assume this role.

If deputies intend to serve a warrant outside Madison County Sheriff's Office jurisdiction, the operations director should provide reasonable advance notice to the applicable agency, request assistance as needed and work cooperatively on operational planning and the mitigation of risks detailed in this policy.

Deputies will remain subject to the policies of the Madison County Sheriff's Office when assisting outside agencies or serving a warrant outside Madison County Sheriff's Office jurisdiction.

607.11 MEDIA ACCESS

No advance information regarding warrant service operations shall be released without the approval of the Sheriff. Any media inquiries or press release after the fact shall be handled in accordance with the Media Relations Policy.

607.12 TRAINING

The Training Supervisor should ensure deputies receive periodic training on this policy and associated topics, such as legal issues, warrant preparation, warrant service and reporting requirements.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Operations Planning and Deconfliction

608.1 PURPOSE AND SCOPE

This policy provides guidelines for planning, deconfliction and execution of high-risk operations.

Additional guidance on planning and serving high-risk warrants is provided in the Warrant Service Policy.

608.1.1 DEFINITIONS

Definitions related to this policy include:

High-risk operations - Operations, including service of search and arrest warrants and sting operations, that are likely to present higher risks than are commonly faced by deputies on a daily basis, including suspected fortified locations, reasonable risk of violence or confrontation with multiple persons, or reason to suspect that persons anticipate the operation.

608.2 POLICY

It is the policy of the Madison County Sheriff's Office to properly plan and carry out high-risk operations, including participation in a regional deconfliction system, in order to provide coordination, enhance the safety of members and the public, decrease the risk of compromising investigations and prevent duplicating efforts.

608.3 OPERATIONS DIRECTOR

The Sheriff will designate a member of this department to be the operations director.

The operations director will develop and maintain a risk assessment form to assess, plan and coordinate operations. This form should provide a process to identify high-risk operations.

The operations director will review risk assessment forms with involved supervisors to determine whether a particular incident qualifies as a high-risk operation. The director will also have the responsibility for coordinating operations that are categorized as high risk.

608.4 RISK ASSESSMENT

608.4.1 RISK ASSESSMENT FORM PREPARATION

Deputies assigned as operational leads for any operation that may qualify as a high-risk operation shall complete a risk assessment form.

When preparing the form, the deputy should query all relevant and reasonably available intelligence resources for information about the subject of investigation, others who may be present and the involved location. These sources may include regional intelligence and criminal justice databases, target deconfliction systems, firearm records, commercial databases and property records. Where appropriate, the deputy should also submit information to these resources.

The deputy should gather available information that includes, but is not limited to:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) Photographs, including aerial photographs, if available, of the involved location, neighboring yards and obstacles.

(b) Maps of the location.

(c) Diagrams of any property and the interior of any buildings that are involved.

(d) Historical information about the subject of investigation (e.g., history of weapon possession or use, known mental illness, known drug use, threats against police, gang affiliation, criminal history).

(e) Historical information about others who may be present at the location (e.g., other criminals, innocent third parties, dependent adults, children, animals).

(f) Obstacles associated with the location (e.g., fortification, booby traps, reinforced doors/windows, surveillance measures, number and type of buildings, geographic and perimeter barriers, the number and types of weapons likely to be present, information that suggests the presence of explosives, chemicals or other hazardous materials, the potential for multiple dwellings or living spaces, availability of keys/door combinations).

(g) Other environmental factors (e.g., nearby venues such as schools and day care centers, proximity of adjacent homes or other occupied buildings, anticipated pedestrian and vehicle traffic at the time of service).

(h) Other available options that may minimize the risk to deputies and others (e.g., making an off-site arrest or detention of the subject of investigation).

608.4.2 RISK ASSESSMENT REVIEW

Deputies will present the threat assessment form and other relevant documents (such as copies of search warrants and affidavits and arrest warrants) to their supervisor and the operations director.

The supervisor and operations director shall confer with the Sheriff and determine the level of risk. Supervisors should take reasonable actions if there is a change in circumstances that elevates the risks associated with the operation.

608.4.3 HIGH-RISK OPERATIONS

If the operations director, after consultation with the Sheriff, determines that the operation is high risk, the operations director should:

(a) Determine what resources will be needed at the location, and contact and/or place on standby any of the following appropriate and available resources:

1. Crisis Response Unit (CRU)
2. Additional personnel
3. Outside agency assistance
4. Special equipment
5. Medical personnel
6. Persons trained in negotiation
7. Additional surveillance

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

8. Canines
9. Property and Evidence Section or analytical personnel to assist with cataloguing seizures
10. Forensic specialists
11. Specialized mapping for larger or complex locations

(b) Contact the appropriate department members or other agencies as warranted to begin preparation.

(c) Ensure that all legal documents such as search warrants are complete and have any modifications reasonably necessary to support the operation.

(d) Coordinate the actual operation.

608.5 DECONFLICTION

Deconfliction systems are designed to identify persons and locations associated with investigations or law enforcement operations and alert participating agencies when others are planning or conducting operations in close proximity or time or are investigating the same individuals, groups or locations.

The deputy who is the operations lead shall ensure the subject of investigation and operations information have been entered in an applicable deconfliction system to determine if there is reported conflicting activity. This should occur as early in the process as practicable, but no later than two hours prior to the commencement of the operation. The deputy should also enter relevant updated information when it is received.

If any conflict is discovered, the supervisor will contact the involved jurisdiction and resolve the potential conflict before proceeding.

608.6 OPERATIONS PLAN

The operations director should ensure that a written operations plan is developed for all high-risk operations. Plans should also be considered for other operations that would benefit from having a formal plan.

The plan should address such issues as:

(a) Operation goals, objectives and strategies.

(b) Operation location and people:

(a) The subject of investigation (e.g., history of weapon possession/use, known mental illness issues, known drug use, threats against police, gang affiliation, criminal history)

(b) The location (e.g., fortification, booby traps, reinforced doors/windows, surveillance cameras and/or lookouts, number/type of buildings, geographic and perimeter barriers, the number and types of weapons likely to be present, information that suggests the presence of explosives, chemicals or other hazardous materials, the potential for multiple dwellings or living spaces,

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

availability of keys/door combinations), including aerial photos, if available, and maps of neighboring yards and obstacles, diagrams and other visual aids

(c) Other environmental factors (e.g., nearby venues such as schools and day care centers, proximity of adjacent homes or other occupied buildings, anticipated pedestrian and vehicle traffic at the time of service)

(d) Identification of other people who may be present in or around the operation, such as other criminal suspects, innocent third parties and children

(c) Information from the threat assessment form by attaching a completed copy in the operational plan.

1. The volume or complexity of the information may indicate that the plan includes a synopsis of the information contained on the threat assessment form to ensure clarity and highlighting of critical information.

(d) Participants and their roles.

1. An adequate number of uniformed deputies should be included in the operation team to provide reasonable notice of a legitimate law enforcement operation.

2. How all participants will be identified as law enforcement.

(e) Whether deconfliction submissions are current and all involved individuals, groups and locations have been deconflicted to the extent reasonably practicable.

(f) Identification of all communications channels and call-signs.

(g) Use of force issues.

(h) Contingencies for handling medical emergencies (e.g., services available at the location, closest hospital, closest trauma center).

(i) Plans for detaining people who are not under arrest.

(j) Contingencies for handling children, dependent adults, animals and other people who might be at the location in accordance with the Child Abuse, Adult Abuse, Child and Dependent Adult Safety and Animal Control policies.

(k) Communications plan

(l) Responsibilities for writing, collecting, reviewing and approving reports.

608.6.1 OPERATIONS PLAN RETENTION

Since the operations plan contains intelligence information and descriptions of law enforcement tactics, it shall not be filed with the report. The operations plan shall be stored separately and retained in accordance with the established records retention schedule.

608.7 OPERATIONS BRIEFING

A briefing should be held prior to the commencement of any high-risk operation to allow all participants to understand the operation, see and identify each other, identify roles and responsibilities and ask questions or seek clarification as needed. Anyone who is not present at the briefing should not respond to the operation location without specific supervisory approval.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) The briefing should include a verbal review of plan elements, using visual aids, to enhance the participants' understanding of the operations plan.

(b) All participants should be provided a copy of the operations plan and search warrant, if applicable. Participating personnel should be directed to read the search warrant and initial a copy that is retained with the operation plan. Any items to be seized should be identified at the briefing.

(c) The operations director shall ensure that all participants are visually identifiable as law enforcement officers.

1. Exceptions may be made by the operations director for deputies who are conducting surveillance or working under cover. However, those members exempt from visual identification should be able to transition to a visible law enforcement indicator at the time of enforcement actions, such as entries or arrests, if necessary.

(d) The briefing should include details of the communications plan.

1. It is the responsibility of the operations director to ensure that the Dispatch Center is notified of the time and location of the operation prior to deputies arriving at the location.

2. If the radio channel needs to be monitored by the Dispatch Center, the dispatcher assigned to monitor the operation may attend the briefing.

3. The briefing should include a communications check to ensure that all participants are able to communicate with the available equipment on the designated radio channel.

608.8 CRU PARTICIPATION

If the operations director determines that CRU participation is appropriate, the director and the CRU supervisor shall work together to develop a written plan. The CRU supervisor shall assume operational control until all persons at the scene are appropriately detained and it is safe to begin a search. When this occurs, the CRU supervisor shall transfer control of the scene to the handling supervisor. This transfer should be communicated to the deputies present.

608.9 MEDIA ACCESS

No advance information regarding planned operations shall be released without the approval of the Sheriff. Any media inquiries or press release after the fact shall be handled in accordance with the Media Relations Policy.

608.10 OPERATIONS DEBRIEFING

High-risk operations should be debriefed as soon as reasonably practicable. The debriefing should include as many participants as possible. This debrief may be separate from any CRU debriefing.

608.11 TRAINING

The Training Supervisor should ensure deputies and CRU team members who participate in operations subject to this policy receive periodic training including, but not limited to, topics such as legal issues, deconfliction practices, operations planning concepts and reporting requirements.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Chapter 7 - Equipment

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Department-Owned and Personal Property

700.1 PURPOSE AND SCOPE

This policy addresses the care of department-owned property and the role of the Department when personal property, the property of another person, or department-owned property is damaged or lost.

700.2 POLICY

Members of the Madison County Sheriff's Office shall properly care for department property assigned or entrusted to them. Department-owned property that becomes damaged shall be promptly replaced. Members' personal property that becomes damaged during the performance of assigned duties will be reimbursed in accordance with this policy.

700.3 DEPARTMENT-ISSUED PROPERTY

All property and equipment issued by the Department shall be documented in the appropriate property sheet or equipment log. Receipt of issued items shall be acknowledged by the receiving member's signature. Upon separation from the Department, all issued property and equipment shall be returned. Documentation of the return shall be acknowledged by the signature of a supervisor.

700.3.1 CARE OF PROPERTY

Members shall be responsible for the safekeeping, serviceable condition, proper care, proper use and replacement of department property that has been assigned or entrusted to them.

Intentional or negligent abuse or misuse of department property may lead to discipline including, but not limited to, the cost of repair or replacement.

(a) Members shall promptly report, through their chain of command, any loss, damage to, or unserviceable condition of any department-issued property or equipment.

1. A supervisor receiving such a report shall conduct an investigation and direct a memo to the appropriate Division Supervisor, which shall include the result of the investigation and whether misconduct or negligence caused the loss, damage or unserviceable condition.
2. A review by command staff should determine whether additional action is appropriate.

(b) The use of damaged or unserviceable property should be discontinued as soon as practicable, and the item replaced with a comparable item as soon as available and following notice to a supervisor.

(c) Except when otherwise directed by competent authority or otherwise reasonable by circumstances, department property shall only be used by those to whom it was assigned. Use should be limited to official purposes and in the capacity for which it was designed.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Department property shall not be thrown away, sold, traded, donated, destroyed or otherwise disposed of without proper authority.

(e) A supervisor’s approval is required before any attempt to repair damaged or unserviceable property is made by a member.

700.4 PERSONAL PROPERTY

Carrying and/or using personal property or equipment on-duty requires prior written approval by the Sheriff or appropriate Division Supervisor. The member should submit a request that includes a description of the property and the reason and length of time it will be used. Personal property of the type routinely carried by persons who are not performing law enforcement duties, and that is not a weapon, is excluded from this requirement.

The Department will not replace or repair costly items (e.g., jewelry, expensive watches, exotic equipment) that are not reasonably required as part of work.

700.4.1 FILING CLAIMS FOR PERSONAL PROPERTY

Claims for reimbursement for damage to, or loss of, personal property must be made on the proper form. This form is submitted to the member's immediate supervisor. The supervisor may require a separate written report.

The supervisor receiving such a report shall investigate and direct a memo to the appropriate Division Supervisor, which shall include the result of the investigation and whether reasonable care was taken to prevent the loss, damage or unserviceable condition.

Upon review by command staff and a finding that no misconduct or negligence was involved, repair or replacement may be recommended by the Sheriff, who will then forward the claim to the County department responsible for issuing payments.

700.5 DAMAGE TO PROPERTY OF ANOTHER PERSON

Anyone who intentionally or unintentionally damages or causes to be damaged the real or personal property of another person while performing any law enforcement function shall promptly report the damage through his/her chain of command.

The supervisor receiving such a report shall conduct an investigation and direct a memo to the appropriate Division Supervisor, which shall include the result of the investigation and whether reasonable care was taken to prevent the loss, damage or unserviceable condition.

A review of the incident by command staff to determine whether misconduct or negligence was involved should be completed.

700.5.1 DAMAGE BY PERSONNEL OF ANOTHER AGENCY

Personnel from another agency may intentionally or unintentionally cause damage to the real or personal property of the County of Madison County, Virginia or of another person while performing their duties within the jurisdiction of this department. It shall be the responsibility of the department member present or the member responsible for the property to report the damage as follows:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) A verbal report shall be made to the member's immediate supervisor as soon as circumstances permit.

(b) A written report shall be submitted before the member goes off-duty or as otherwise directed by the supervisor.

The supervisor receiving such a report shall conduct an investigation and direct a memo to the appropriate Division Supervisor, which shall include the result of the investigation and whether misconduct or negligence caused the loss, damage or unserviceable condition.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Personal Communication Devices

701.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the use of mobile telephones and communication devices, whether issued by the Department or personally owned, while on-duty or when used for authorized work-related purposes.

This policy generically refers to all such devices as Personal Communication Devices (PCDs) but is intended to include all mobile telephones, personal digital assistants (PDAs), wireless capable tablets, and similar wireless two-way communications and/or portable internet access devices. PCD use includes but is not limited to placing and receiving calls, text messaging, blogging and microblogging, emailing, using video or camera features, playing games, and accessing sites or services on the internet.

701.2 POLICY

The Madison County Sheriff's Office allows members to utilize department-issued PCDs and to possess personally owned PCDs in the workplace, subject to certain limitations. Any PCD used while on-duty, or used off-duty in any manner reasonably related to the business of the Department, will be subject to monitoring and inspection consistent with the standards set forth in this policy.

The inappropriate use of a PCD while on-duty may impair officer safety. Additionally, members are advised and cautioned that the use of a personally owned PCD either on-duty or after duty hours for business-related purposes may subject the member and the member's PCD records to civil or criminal discovery or disclosure under the Virginia Freedom of Information Act.

Members who have questions regarding the application of this policy or the guidelines contained herein are encouraged to seek clarification from supervisory staff.

701.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to any communication accessed, transmitted, received or reviewed on any PCD issued or funded by the Department and shall have no expectation of privacy in their location should the device be equipped with location detection capabilities (see the Information Technology Use Policy for additional guidance).

701.4 DEPARTMENT-ISSUED PCD

Depending on a member's assignment and the needs of the position, the Department may, at its discretion, issue a PCD for the member's use to facilitate on-duty performance. Department-issued PCDs may not be used for personal business either on- or off-duty unless authorized by the Sheriff or the authorized designee. Such devices and the associated telephone number, if any, shall remain the sole property of the Department and shall be subject to inspection or monitoring (including all related records and content) at any time without notice and without cause.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Personal Communication Devices

Unless a member is expressly authorized by the Sheriff or the authorized designee for off-duty use of the PCD, the PCD will either be secured in the workplace at the completion of the tour of duty or will be turned off when leaving the workplace.

701.5 PERSONALLY OWNED PCD

Members may carry a personally owned PCD while on-duty, subject to the following conditions and limitations:

(a) Permission to carry a personally owned PCD may be revoked if it is used contrary to provisions of this policy.

(b) The Department accepts no responsibility for loss of or damage to a personally owned PCD.

(c) The PCD and any associated services shall be purchased, used and maintained solely at the member's expense.

(d) The device should not be used for work-related purposes except in exigent circumstances (e.g., unavailability of radio communications). Members will have a reduced expectation of privacy when using a personally owned PCD in the workplace and have no expectation of privacy with regard to any department business-related communication.

(e) The device shall not be utilized to record or disclose any department business-related information, including photographs, video or the recording or transmittal of any information or material obtained or made accessible as a result of employment or appointment with the Department, without the express authorization of the Sheriff or the authorized designee.

(f) Use of a personally owned PCD while at work or for work-related business constitutes consent for the Department to access the PCD to inspect and copy data to meet the needs of the Department, which may include litigation, retention and release obligations and internal investigations. If the PCD is carried on-duty, members will provide the Department with the telephone number of the device.

(g) All work-related documents, emails, photographs, recordings or other public records created or received on a member's personally owned PCD should be transferred to the Madison County Sheriff's Office and deleted from the member's PCD as soon as reasonably practicable but no later than the end of the member's shift.

Except with prior express authorization from their supervisors, members are not obligated or required to carry, access, monitor or respond to electronic communications using a personally owned PCD while off-duty. If a member is in an authorized status that allows for appropriate compensation consistent with policy or if the member has prior express authorization from his/her supervisor, the member may engage in department business-related communications. Should members engage in such approved off-duty communications or work, members entitled to compensation shall promptly document the time worked and communicate the information to their

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

supervisors to ensure appropriate compensation. Members who independently document off-duty department-related business activities in any manner shall promptly provide the Department with a copy of such records to ensure accurate record keeping.

701.6 USE OF PCD

The following protocols shall apply to all PCDs that are carried while on-duty or used to conduct department business:

(a) A PCD shall not be carried in a manner that allows it to be visible while in uniform, unless it is in an approved carrier.

(b) All PCDs in the workplace shall be set to silent or vibrate mode.

(c) A PCD may not be used to conduct personal business while on-duty, except for brief personal communications (e.g., informing family of extended hours). Members shall endeavor to limit their use of PCDs to authorized break times, unless an emergency exists.

(d) Members may use a PCD to communicate with other personnel in situations where the use of radio communications is either impracticable or not feasible. PCDs should not be used as a substitute for, as a way to avoid, or in lieu of regular radio communications.

(e) Members are prohibited from taking pictures, audio or video recordings or making copies of any such picture or recording media unless it is directly related to official department business. Disclosure of any such information to any third party through any means, without the express authorization of the Sheriff or the authorized designee, may result in discipline.

(f) Members will not access social networking sites for any purpose that is not official department business.

(g) Using PCDs to harass, threaten, coerce or otherwise engage in inappropriate conduct with any third party is prohibited. Any member having knowledge of such conduct shall promptly notify a supervisor.

701.7 SUPERVISOR RESPONSIBILITIES

The responsibilities of supervisors include, but are not limited to:

(a) Ensuring that members under their command are provided appropriate training on the use of PCDs consistent with this policy.

(b) Monitoring, to the extent practicable, PCD use in the workplace and taking prompt corrective action if a member is observed or reported to be improperly using a PCD.

    1. An investigation into improper conduct should be promptly initiated when circumstances warrant.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. Before conducting any administrative search of a member's personally owned device, supervisors should consult with the Sheriff or the authorized designee.

701.8 OFFICIAL USE

Members are reminded that PCDs are not secure devices and conversations may be intercepted or overheard. Caution should be exercised while utilizing PCDs to ensure that sensitive information is not inadvertently transmitted. As soon as reasonably possible, members shall conduct sensitive or private communications on a land-based or other department communications network.

701.9 USE WHILE DRIVING

The use of a PCD while driving can adversely affect safety, cause unnecessary distractions, and present a negative image to the public. Except for reporting emergencies, state law generally prohibits anyone operating a motor vehicle from holding a PCD; however, it permits the use of a PCD by a deputy operating a law enforcement vehicle while engaged in the performance of his/her official duties (Va. Code § 46.2-818.2). Deputies should restrict the use of these devices to matters of an urgent nature and should, where practicable, stop the vehicle at an appropriate location to use the PCD.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Vehicle Maintenance

702.1 PURPOSE AND SCOPE

The purpose of this policy is to ensure that department vehicles are appropriately maintained.

702.2 POLICY

The Madison County Sheriff's Office will service department vehicles to ensure they remain operational and maintain their appearance, as resources allow.

702.3 GENERAL DUTIES

Members are responsible for assisting in maintaining department vehicles so that they are properly equipped, properly maintained and properly refueled and present a clean appearance.

702.4 DEFECTIVE VEHICLES

When a vehicle becomes inoperative or in need of repair that affects the safety of the vehicle, that vehicle shall be removed from service. Proper documentation shall be promptly completed by the member who becomes aware of the defective condition and forwarded for action.

Documents describing the correction of the safety issue shall be promptly filed with the vehicle history.

702.4.1 DAMAGE OR POOR PERFORMANCE

Vehicles that may have been damaged or perform poorly shall be removed from service for inspections and repairs as soon as practicable.

702.4.2 SEVERE USE

Vehicles operated under severe-use conditions, which include operations for which the vehicle is not designed or that exceed the manufacturer’s parameters, should be removed from service and subjected to a safety inspection as soon as practicable. Such conditions may include rough roadway or off-road driving, hard or extended braking, pursuits or prolonged high-speed operation.

702.4.3 REMOVAL OF WEAPONS

All firearms, weapons, and control devices shall be removed from a vehicle and properly secured.

702.5 VEHICLE EQUIPMENT

Certain items shall be maintained in all department vehicles.

702.5.1 PATROL VEHICLES

Patrol vehicles must be clearly marked, have a functioning siren and emergency lights and have a communications system enabling communication with other members of the Madison County Sheriff's Office at all times.

Deputies shall inspect the patrol vehicle at the beginning of the shift and ensure that the following equipment, at a minimum, is in the vehicle:

- 20 emergency road flares

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

- 2 sticks yellow crayon or chalk
- 1 roll crime scene barricade tape
- 1 first-aid kit and CPR mask
- 1 blanket
- 1 fire extinguisher
- 1 bloodborne pathogen kit, including protective gloves and a National Institute for Occupational Safety and Health (NIOSH) particulate respirator mask
- 1 sharps container
- 1 hazardous waste disposal bag
- 1 high-visibility vest
- 1 hazardous materials emergency response handbook
- 1 evidence collection kit
- 1 camera
- Spare tire, jack and lug wrench
- Rain gear

702.5.2 UNMARKED VEHICLES

Members driving unmarked department vehicles shall ensure that the following equipment, at a minimum, is in the vehicle:

- 20 emergency road flares
- 1 roll crime scene barricade tape
- 1 first-aid kit and CPR mask
- 1 blanket
- 1 bloodborne pathogen kit, including protective gloves and NIOSH particulate respirator mask
- 1 sharps container
- 1 hazardous waste disposal bag
- 1 high-visibility vest
- 1 hazardous materials emergency response handbook
- 1 evidence collection kit
- 1 camera
- Spare tire, jack, and lug wrench
- Rain gear

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

702.6 VEHICLE REFUELING

Absent emergency conditions or supervisor approval, patrol vehicles shall not be placed into service with less than one-quarter tank of fuel. Patrol vehicles should not be retired at the end of shift with less than one-quarter tank of fuel. Vehicles shall only be refueled at the authorized location.

702.7 WASHING OF VEHICLES

Vehicles shall be kept clean at all times and, weather conditions permitting, shall be washed as necessary to maintain the professional appearance of the Department.

Patrol deputies shall obtain clearance from the dispatcher before going to the car wash. Only one patrol vehicle should be at the car wash at a time unless otherwise approved by a supervisor.

Members using a vehicle shall remove any trash or debris at the end of their shifts. Confidential material should be placed in a designated receptacle that has been provided for shredding this material.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Vehicle Use

703.1 PURPOSE AND SCOPE

The purpose of this policy is to establish a system of accountability to ensure department vehicles are used appropriately. This policy provides guidelines for on- and off-duty use of department vehicles and shall not be construed to create or imply any contractual obligation by the County of Madison County, Virginia to provide assigned take-home vehicles.

703.2 POLICY

The Madison County Sheriff's Office provides vehicles for department-related business and may assign patrol and unmarked vehicles based on a determination of operational efficiency, economic impact to the Department, requirements for tactical deployments and other considerations.

703.3 USE OF VEHICLES

703.3.1 SHIFT ASSIGNED VEHICLES

The Shift Supervisor shall ensure a copy of the shift assignment roster, indicating member assignments and vehicle numbers, is completed for each shift and retained in accordance with the established records retention schedule. If a member exchanges vehicles during his/her shift, the new vehicle number shall be documented on the roster.

703.3.2 OTHER USE OF VEHICLES

Members utilizing a vehicle for any purpose other than their normally assigned duties or normal vehicle assignment (e.g., transportation to training, community event) shall first notify the Shift Supervisor. A notation will be made on the shift assignment roster indicating the member’s name and vehicle number.

This subsection does not apply to those who are assigned to transport vehicles to and from the maintenance yard or car wash.

703.3.3 INSPECTIONS

Members shall be responsible for inspecting the interior and exterior of any assigned vehicle before taking the vehicle into service and at the conclusion of their shifts. Any previously unreported damage, mechanical problems, unauthorized contents or other problems with the vehicle shall be promptly reported to a supervisor and documented as appropriate.

The interior of any vehicle that has been used to transport any person other than a member of this department should be inspected prior to placing another person in the vehicle and again after the person is removed. This is to ensure that unauthorized or personal items have not been left in the vehicle.

When transporting any suspect, prisoner or arrestee, the transporting member shall search all areas of the vehicle that are accessible by the person before and after that person is transported.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Vehicle Use

All department vehicles are subject to inspection and/or search at any time by a supervisor without notice and without cause. No member assigned to or operating such vehicle shall be entitled to any expectation of privacy with respect to the vehicle or its contents.

703.3.4 SECURITY AND UNATTENDED VEHICLES

Unattended vehicles should be locked and secured at all times. No key should be left in the vehicle except when it is necessary that the vehicle be left running (e.g., continued activation of emergency lights, canine safety, equipment charging). Deputies who exit a vehicle rapidly in an emergency situation or to engage in a foot pursuit must carefully balance the need to exit the vehicle quickly with the need to secure the vehicle.

Members shall ensure all weapons are secured while the vehicle is unattended.

703.3.5 MOBILE DIGITAL TERMINAL

Members assigned to vehicles equipped with a Mobile Data Computer (MDT) shall log onto the MDT with the required information when going on-duty. If the vehicle is not equipped with a working MDT, the member shall notify the Dispatch Center. Use of the MDT is governed by the Mobile Data Computer Use Policy.

703.3.6 VEHICLE LOCATION SYSTEM

Patrol and other vehicles, at the discretion of the Sheriff, may be equipped with a system designed to track the vehicle's location. While the system may provide vehicle location and other information, members are not relieved of their responsibility to use required communication practices to report their location and status.

Members shall not make any unauthorized modifications to the system. At the start of each shift, members shall verify that the system is on and report any malfunctions to their supervisor. If the member finds that system is not functioning properly at any time during the shift he/she should exchange the vehicle for one with a working system, if available.

System data may be accessed by supervisors at any time. However, access to historical data by personnel other than supervisors will require Division Supervisor approval.

All data captured by the system shall be retained in accordance with the established records retention schedule.

703.3.7 KEYS

Members approved to operate marked patrol vehicles should be issued a copy of the key as part of their initial equipment distribution. Members who are assigned a specific vehicle should be issued keys for that vehicle.

Members shall not duplicate keys. The loss of a key shall be promptly reported in writing through the member's chain of command.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

703.3.8 AUTHORIZED PASSENGERS

Members operating department vehicles shall not permit persons other than County personnel or persons required to be conveyed in the performance of duty, or as otherwise authorized, to ride as passengers in the vehicle, except as stated in the Ride-Alongs Policy.

703.3.9 ALCOHOL

Members who have consumed alcohol are prohibited from operating any department vehicle unless it is required by the duty assignment (e.g., task force, undercover work). Regardless of assignment, members may not violate state law regarding vehicle operation while intoxicated.

703.3.10 PARKING

Except when responding to an emergency or when urgent department-related business requires otherwise, members driving department vehicles should obey all parking regulations at all times.

Department vehicles should be parked in assigned stalls. Members shall not park privately owned vehicles in stalls assigned to department vehicles or in other areas of the parking lot that are not so designated unless authorized by a supervisor. Privately owned motorcycles shall be parked in designated areas.

703.3.11 ACCESSORIES AND/OR MODIFICATIONS

There shall be no modifications, additions or removal of any equipment or accessories without written permission from the assigned vehicle program manager.

703.3.12 NON-SWORN MEMBER USE

Non-sworn members using marked emergency vehicles shall ensure that all weapons have been removed before going into service. Non-sworn members shall prominently display the “out of service” placards or light bar covers at all times. Non-sworn members shall not operate the emergency lights or siren of any vehicle unless expressly authorized by a supervisor.

703.4 INDIVIDUAL MEMBER ASSIGNMENT TO VEHICLES

Department vehicles may be assigned to individual members at the discretion of the Sheriff. Vehicles may be assigned for on-duty and/or take-home use. Assigned vehicles may be changed at any time. Permission to take home a vehicle may be withdrawn at any time.

The assignment of vehicles may be suspended when the member is unable to perform his/her regular assignment.

703.4.1 ON-DUTY USE

Vehicle assignments shall be based on the nature of the member’s duties, job description and essential functions, and employment or appointment status. Vehicles may be reassigned or utilized by other department members at the discretion of the Sheriff or the authorized designee.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

703.4.2 UNSCHEDULED TAKE-HOME USE

Circumstances may arise where department vehicles must be used by members to commute to and from a work assignment. Members may take home department vehicles only with prior approval of a supervisor and shall meet the following criteria:

(a) The circumstances are unplanned and were created by the needs of the Department.

(b) Other reasonable transportation options are not available.

(c) The member lives within a reasonable distance (generally not to exceed a 60-minute drive time) of the Madison County, Virginia County limits.

(d) Off-street parking will be available at the member’s residence.

(e) The vehicle will be locked when not attended.

(f) All firearms, weapons and control devices will be removed from the interior of the vehicle and properly secured in the residence when the vehicle is not attended, unless the vehicle is parked in a locked garage.

703.4.3 ASSIGNED VEHICLES

Assignment of take-home vehicles shall be based on the location of the member's residence; the nature of the member's duties, job description and essential functions; and the member's employment or appointment status. Deputies must reside within a 25-minute commute from their residence to the county line. Members who reside outside the County of Madison County, Virginia may be required to secure the vehicle at a designated location or the Department at the discretion of the Sheriff.

Department members shall sign a take-home vehicle agreement that outlines certain standards, including, but not limited to, how the vehicle shall be used, where it shall be parked when the member is not on-duty, vehicle maintenance responsibilities and member enforcement actions.

Members are cautioned that under federal and local tax rules, personal use of a County vehicle may create an income tax liability for the member. Questions regarding tax rules should be directed to the member's tax adviser.

Criteria for use of take-home vehicles include the following:

(a) Vehicles shall only be used for work-related purposes and shall not be used for personal errands or transports, unless special circumstances exist and the Sheriff or a Division Supervisor gives authorization.

(b) Vehicles may be used to transport the member to and from the member's residence for work-related purposes.

(c) Vehicles will not be used when off-duty except:

1. In circumstances when a member has been placed on call by the Sheriff or Division Supervisors and there is a high probability that the member will be called back to duty.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. When the member is performing a work-related function during what normally would be an off-duty period, including vehicle maintenance or travelling to or from a work-related activity or function.
3. When the member has received permission from the Sheriff or Division Supervisors.
4. When the vehicle is being used by the Sheriff, Division Supervisors or members who are in on-call administrative positions.
5. When the vehicle is being used by on-call investigators.

(d) While operating the vehicle, authorized members will carry and have accessible their duty firearms and be prepared to perform any function they would be expected to perform while on-duty.

(e) The two-way communications radio, MDT and global positioning satellite device, if equipped, must be on and set to an audible volume when the vehicle is in operation.

(f) Unattended vehicles are to be locked and secured at all times.

1. No key should be left in the vehicle except when it is necessary that the vehicle be left running (e.g., continued activation of emergency lights, canine safety, equipment charging).
2. All weapons shall be secured while the vehicle is unattended.
3. All department identification, portable radios and equipment should be secured.

(g) Vehicles are to be parked off-street at the member's residence unless prior arrangements have been made with the Sheriff or the authorized designee. If the vehicle is not secured inside a locked garage, all firearms and kinetic impact weapons shall be removed and properly secured in the residence, or secured inside the locked vehicle in a locked weapons rack or trunk compartment. (see the Firearms Policy regarding safe storage of firearms at home).

(h) Vehicles are to be secured at the member's residence or the appropriate department facility, at the discretion of the Department, when a member will be away (e.g., on vacation) for periods exceeding one week.

1. If the vehicle remains at the residence of the member, the Department shall have access to the vehicle.
2. If the member is unable to provide access to the vehicle, it shall be parked at the Department.

(i) The member is responsible for the care and maintenance of the vehicle.

703.4.4 ENFORCEMENT ACTIONS

When driving a take-home vehicle to and from work outside of the jurisdiction of the Madison County Sheriff's Office or while off-duty, a deputy shall not initiate enforcement actions except in those circumstances where a potential threat to life or serious property damage exists (see the Off-Duty Law Enforcement Actions and Law Enforcement Authority policies).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Deputies may render public assistance when it is deemed prudent (e.g., to a stranded motorist).

Deputies driving take-home vehicles shall be armed and appropriately attired and shall carry their department-issued identification. Deputies should also ensure that department radio communication capabilities are maintained to the extent feasible.

703.4.5 MAINTENANCE

Members are responsible for the cleanliness (exterior and interior) and overall maintenance of their assigned vehicles. Cleaning and maintenance supplies will be provided by the Department. Failure to adhere to these requirements may result in discipline and loss of vehicle assignment. The following should be performed as outlined below:

(a) Members shall make daily inspections of their assigned vehicles for service/ maintenance requirements and damage.

(b) It is the member's responsibility to ensure that his/her assigned vehicle is maintained according to the established service and maintenance schedule.

(c) All scheduled vehicle maintenance and car washes shall be performed as necessary at a facility approved by the department supervisor in charge of vehicle maintenance.

(d) The Department shall be notified of problems with the vehicle and approve any major repairs before they are performed.

(e) When leaving the vehicle at the maintenance facility, the member will inform the mechanic of the work to be done.

(f) All weapons shall be removed from any vehicle left for maintenance.

(g) Supervisors shall make, at a minimum, monthly inspections of vehicles assigned to members under their command to ensure the vehicles are being maintained in accordance with this policy.

703.5 UNMARKED VEHICLES

Unmarked vehicles are assigned to various divisions and their use is restricted to the respective division and the assigned member, unless otherwise approved by a supervisor. Any member operating an unmarked vehicle shall record vehicle usage on the sign-out log maintained in the division for that purpose. Any use of unmarked vehicles by those who are not assigned to the division to which the vehicle is assigned shall also be recorded with the Shift Supervisor on the shift assignment roster.

703.6 DAMAGE, ABUSE AND MISUSE

When any department vehicle is involved in a traffic accident or otherwise incurs damage, the involved member shall promptly notify a supervisor. Any traffic accident report shall be filed with the agency having jurisdiction (see the Traffic Accidents Policy).

Damage to any department vehicle that was not caused by a traffic accident shall be immediately reported during the shift in which the damage was discovered and documented in memorandum format, which shall be forwarded to the Shift Supervisor. An administrative investigation should be initiated to determine if there has been any vehicle abuse or misuse.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

703.7 TOLL ROAD USAGE

Law enforcement vehicles are exempt from incurring toll lane charges when (Va. Code § 33.2-500 et seq.):

(a) Responding to an emergency incident.

(b) Patrolling high-occupancy toll (HOT) lanes pursuant to an agreement by a state agency and the HOT lane operator.

(c) Engaged in a time-sensitive investigation, active surveillance or actual pursuit of persons who are known or suspected to be engaged in, or who have knowledge of, criminal activity.

Members operating department vehicles for any reason other than those exempted by law shall pay the appropriate toll charge or utilize the appropriate toll way transponder (Va. Code § 33.2-500 et seq.).

703.8 ATTIRE AND APPEARANCE

When operating any department vehicle while off-duty, members may dress in a manner appropriate for their intended activity. Whenever in view of or in contact with the public, attire and appearance, regardless of the activity, should be suitable to reflect positively upon the Department.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Fiscal Management

704.1 PURPOSE AND SCOPE

This policy provides guidelines to ensure department members handle fiscal matters appropriately in the performance of their duties.

This policy does not address cash-handling issues specific to the Property and Evidence Section and Informants policies.

704.2 POLICY

It is the policy of the Madison County Sheriff's Office to properly manage and audit fiscal operations including budget preparation, cash transactions, fund expenditures and disposition of assets, and to maintain accurate records of fiscal transactions in order to protect the integrity of department operations and ensure the public trust.

704.3 FISCAL MANAGEMENT

The Sheriff shall designate a person as the fiscal manager responsible for maintaining and managing fiscal operations.

Each member overseeing a fiscal responsibility is required to create and maintain an accurate and current transaction ledger that is approved by the fiscal manager and that documents all transactions relating to the specific fund or fiscal responsibility.

The Department’s accounting system should detail all fiscal operations. The fiscal manager should review all account activities on a monthly basis. The accounting system should provide a continuous and accurate update of the following:

(a) Initial appropriations for each account program.

(b) Account balance after each expenditure.

(c) Documentation of all expenditures and encumbrances.

(d) A statement of the account’s unencumbered balance.

704.3.1 CASH MANAGEMENT

All cash funds shall be properly collected, safeguarded and disbursed by the assigned member under the direction of the County Treasurer. The assigned member shall:

(a) Maintain a system or record of appropriations among organizational components.

(b) Prepare financial statements, including quarterly reports.

(c) Conduct internal audits.

(d) Ensure that external audits are conducted as required.

(e) Verify members or positions authorized to accept or disburse funds.

(f) Prepare receipts or other documentation for disbursed funds.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

704.3.2 MINIMUM HANDLING PROCEDURES

The Sheriff should designate one or more members of the Department to oversee the handling of all cash funds. Any designated member is responsible for establishing procedures to include, at a minimum:

(a) A balance sheet, ledger, or other system that identifies initial balance, credits (cash income received), debits (cash disbursed), and the balance on hand.

(b) Receipts or documentation for cash received.

(c) Authorization for cash disbursement, including Sheriff authorization for expenses in excess of a minimum specified amount, unless already specifically designated by policy.

(d) Records, documentation, or invoice requirements for cash expenditures.

(e) Members authorized to disburse or accept cash.

(f) Quarterly accounting of all cash activities.

(g) An independent audit of the department's fiscal activities.

704.4 FISCAL TRANSACTIONS

Each member overseeing a fiscal responsibility shall document all transactions on the ledger and any other appropriate forms. Each person participating in the transaction shall sign or otherwise validate the ledger, attesting to the accuracy of the entry. Transactions should include the filing of an appropriate receipt, invoice, cash transfer form or expense report.

704.5 ROUTINE CASH HANDLING

Members who handle cash as part of their regular duties (e.g., evidence technicians, the Investigations supervisor, those who accept payment for department services) will discharge those duties in accordance with the procedures established for those tasks (see the Property and Evidence Section and Informants policies).

704.6 OTHER CASH HANDLING

Members who, within the course of their duties, are in possession of cash that is not their property or that is outside their defined cash-handling responsibilities shall, as soon as practicable, verify the amount, summon another member to verify their accounting, and process the cash for safekeeping or as evidence or found property, in accordance with the Property and Evidence Section Policy.

Cash in excess of $1,000 requires immediate notification of a supervisor, special handling, verification and accounting by the supervisor. Each member involved in this process shall complete an appropriate report or record entry.

704.7 AUDITS

Each Division Supervisor shall monitor fiscal activities and the budget related to his/her area of responsibility using a procedure and forms approved by the fiscal manager. Internal control

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

procedures shall be established and shall include evaluation of staff member's fiscal management functions. Any discrepancies shall be immediately reported to the fiscal manager and the Sheriff.

The fiscal manager shall ensure that an annual independent audit is conducted of the accounts and finances of the Department. All department funds shall be open for inspection and audit by auditors at any time. Members of the Department shall cooperate fully and provide assistance in support of any audit.

A separate audit of each fund or other fiscal area of responsibility should be completed on a random date, approximately once each year, by the Sheriff or the County.

Audits shall include a review of procedures in place to manage the funds.

704.8 INVENTORY CONTROL OF PROPERTY, EQUIPMENT AND OTHER ASSETS

Members overseeing a fiscal responsibility for the acquisition, management or distribution of any capital or major items of equipment; the issue of any equipment and supplies; or the assignment of control numbers and proper markings are responsible for compliance with inventory control procedures. Such members are also responsible for ensuring:

(a) Required inventory verification is performed in compliance with a process authorized by the fiscal manager.

(b) Appropriate documentation in compliance with a process authorized by the fiscal manager and inclusion in inventory of items purchased or obtained for use by the Department.

(c) Appropriate documentation and deletion from inventory of items properly authorized for disposal by the fiscal manager or the Sheriff.

(d) Reporting and disposition of damaged, excess and surplus property in compliance with a process authorized by the fiscal manager.

(e) Maintenance of complete records for all department property, equipment and other assets.

704.9 PURCHASING

All purchasing of department supplies and equipment will be in compliance with the County purchasing manual and in compliance with a process authorized by the fiscal manager.

Small-item or emergency purchases or rental of equipment during periods when normal purchasing procedures cannot be followed will be in compliance with a process authorized by the fiscal manager.

All purchases for the County made by an employee will require submission of a receipt and appropriate documentation necessary for reimbursement and will be in compliance with a process authorized by the fiscal manager.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Personal Protective Equipment

705.1 PURPOSE AND SCOPE

This policy identifies the different types of personal protective equipment (PPE) provided by the Department as well the requirements and guidelines for the use of PPE.

This policy does not address ballistic vests or protection from communicable disease, as those issues are addressed in the Body Armor and Communicable Diseases policies.

705.1.1 DEFINITIONS

Definitions related to this policy include:

Personal protective equipment (PPE) - Equipment that protects a person from serious workplace injuries or illnesses resulting from contact with chemical, radiological, physical, electrical, mechanical or other workplace hazards.

Respiratory PPE - Any device that is worn by the user to protect from exposure to atmospheres where there is smoke, low levels of oxygen, high levels of carbon monoxide, or the presence of toxic gases or other respiratory hazards. For purposes of this policy, respiratory PPE does not include particulate-filtering masks such as N95 or N100 masks.

705.2 POLICY

The Madison County Sheriff's Office endeavors to protect members by supplying certain PPE to members as provided in this policy.

705.3 DEPUTY RESPONSIBILITIES

Members are required to use PPE as provided in this policy and pursuant to their training.

Members are responsible for proper maintenance and storage of issued PPE. PPE should be stored in an appropriate location so that it is available when needed.

Any member who identifies hazards in the workplace is encouraged to utilize the procedures in the Illness and Injury Prevention Policy to recommend new or improved PPE or additional needs for PPE.

705.4 HEARING PROTECTION

Approved hearing protection shall be used by members during firearms training.

Hearing protection shall meet or exceed the requirements provided in 29 CFR 1910.95 and 16 VAC 25-90-1910.

705.5 EYE PROTECTION

Approved eye protection, including side protection, shall be used by members during firearms training. Eye protection for members who wear prescription lenses shall incorporate the prescription (e.g., eye protection that can be worn over prescription lenses). Members shall ensure their eye protection does not interfere with the fit of their hearing protection.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

The Rangemaster shall ensure eye protection meets or exceeds the requirements provided in 29 CFR 1910.95 and 16 VAC 25-90-1910.

705.6 HEAD AND BODY PROTECTION

Members who make arrests or control crowds should be provided ballistic head protection with an attachable face shield.

Padded body protection consisting of chest, arm, leg and groin protection should be provided as required by any employment agreement.

705.7 RESPIRATORY PROTECTION

The Administration Division Supervisor is responsible for ensuring a respiratory protection plan is developed and maintained by a trained and qualified member. The plan shall include procedures for (29 CFR 1910.134; 16 VAC 25-90-1910:

(a) Selecting appropriate respiratory PPE based on hazards and risks associated with functions or positions.

(b) Fit testing, including identification of members or contractors qualified to conduct fit testing.

(c) Medical evaluations.

(d) PPE inventory control.

(e) PPE issuance and replacement.

(f) Cleaning, disinfecting, storing, inspecting, repairing, discarding and otherwise maintaining respiratory PPE, including schedules for these activities.

(g) Regularly reviewing the PPE plan.

(h) Remaining current with applicable National Institute for Occupational Safety and Health (NIOSH), American National Standards Institute (ANSI), Occupational Safety and Health Administration (OSHA), Environmental Protective Agency (EPA) and state PPE standards and guidelines.

705.7.1 RESPIRATORY PROTECTION USE

Designated members may be issued respiratory PPE based on the member’s assignment (e.g., a narcotics investigator who is involved in clandestine lab investigations).

Respiratory PPE may be worn when authorized by a scene commander who will determine the type and level of protection appropriate at a scene based upon an evaluation of the hazards present.

Scene commanders are responsible for monitoring members using respiratory PPE and their degree of exposure or stress. When there is a change in work area conditions or when a member’s degree of exposure or stress may affect respirator effectiveness, the scene commander shall reevaluate the continued effectiveness of the respirator and direct the member to leave the respirator use area when the scene commander reasonably believes (29 CFR 1910.134; 16 VAC 25-90-1910):

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) It is necessary for the member to wash his/her face and the respirator facepiece to prevent eye or skin irritation associated with respirator use.

(b) The member detects vapor or gas breakthrough, or there is a change in breathing resistance or leakage of the facepiece.

(c) The member needs to replace the respirator, filter, cartridge or canister.

705.7.2 MEMBER RESPONSIBILITIES FOR RESPIRATORY PROTECTION

Members shall not use self-contained breathing apparatus (SCBA), full-face respirators or cartridge respirators unless they have completed training requirements for the equipment.

Members exposed to environments that are reasonably known to be harmful due to gases, smoke or vapors shall use respiratory PPE.

Members using respiratory PPE shall (29 CFR 1910.134; 16 VAC 25-90-1910):

(a) Ensure that they have no facial hair between the sealing surface of the facepiece and the face that could interfere with the seal or the valve function. Members also shall ensure that they have no other condition that will interfere with the face-to-facepiece seal or the valve function.

(b) Not wear corrective glasses, goggles or other PPE that interferes with the seal of the facepiece to the face, or that has not been previously tested for use with that respiratory equipment.

(c) Perform a user seal check per department-approved procedures recommended by the respirator manufacturer each time they put on a tight-fitting respirator.

(d) Leave a respiratory use area whenever they detect vapor or gas breakthrough, changes in breathing resistance or leakage of their facepiece and ensure that the respirator is replaced or repaired before returning to the affected area.

705.7.3 GAS MASK

Full-face air-purifying respirators, commonly referred to as gas masks, may be fitted with mechanical pre-filters or combination cartridge/filter assemblies for use in areas where gases, vapors, dusts, fumes or mists are present. Members must identify and use the correct cartridge based on the circumstances (29 CFR 1910.134; 16 VAC 25-90-1910).

A scene commander may order the use of gas masks in situations where the use of a SCBA is not necessary. These incidents may include areas where tear gas has or will be used or where a vegetation fire is burning. Gas masks shall not be used if there is a potential for an oxygen-deficient atmosphere.

Members shall ensure their gas mask filters are replaced whenever:

(a) They smell, taste or are irritated by a contaminant.

(b) They experience difficulty breathing due to filter loading.

(c) The cartridges or filters become wet.

(d) The expiration date on the cartridges or canisters has been reached.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

705.7.4 SELF-CONTAINED BREATHING APPARATUS

Scene commanders may direct members to use SCBA when entering an atmosphere that may pose an immediate threat to life, would cause irreversible adverse health effects or would impair an individual's ability to escape from a dangerous atmosphere. These situations may include, but are not limited to:

(a) Entering the hot zone of a hazardous materials incident.

(b) Entering any area where contaminant levels may become unsafe without warning, or any situation where exposures cannot be identified or reasonably estimated.

(c) Entering a smoke- or chemical-filled area.

The use of SCBA should not cease until approved by a scene commander.

705.7.5 RESPIRATOR FIT TESTING

No member shall be issued respiratory PPE until a proper fit testing has been completed by a designated member or contractor (29 CFR 1910.134; 16 VAC 25-90-1910).

After initial testing, fit testing for respiratory PPE shall be repeated (29 CFR 1910.134; 16 VAC 25-90-1910):

(a) At least once every 12 months.

(b) Whenever there are changes in the type of SCBA or facepiece used.

(c) Whenever there are significant physical changes in the user (e.g., obvious change in body weight, scarring of the face seal area, dental changes, cosmetic surgery or any other condition that may affect the fit of the facepiece seal).

All respirator fit testing shall be conducted in negative-pressure mode.

705.7.6 RESPIRATORY MEDICAL EVALUATION QUESTIONNAIRE

No member shall be issued respiratory protection that forms a complete seal around the face until (29 CFR 1910.134; 16 VAC 25-90-1910):

(a) The member has completed a medical evaluation that includes a medical evaluation questionnaire.

(b) A physician or other licensed health care professional has reviewed the questionnaire.

(c) The member has completed any physical examination recommended by the reviewing physician or health care professional.

705.8 RECORDS

The Training Supervisor is responsible for maintaining records of all:

(a) PPE training.

(b) Initial fit testing for respiratory protection equipment.

(c) Annual fit testing.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Respirator medical evaluation questionnaires and any subsequent physical examination results.

1. These records shall be maintained in a separate confidential medical file.

The records shall be maintained in accordance with the established records retention schedule (29 CFR 1910.1020; 16 VAC 25-90-1910).

705.9 TRAINING

Members should be trained in the respiratory and other hazards to which they may be potentially exposed during routine and emergency situations.

All members shall be trained in the proper use and maintenance of PPE issued to them, including when the use is appropriate; how to put on, remove and adjust PPE; how to care for the PPE; and the limitations (29 CFR 1910.132; 16 VAC 25-90-1910).

Members issued respiratory PPE shall attend annual training on the proper use of respiratory protection devices (29 CFR 1910.134; 16 VAC 25-90-1910).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Chapter 8 - Support Services

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Crime Analysis

800.1 PURPOSE AND SCOPE

This policy provides guidelines for utilizing crime analysis to support the overall law enforcement efforts of the Madison County Sheriff's Office. It addresses the collection and dissemination of crime analysis data that is useful to long-range planning and that can assist in identifying enforcement priorities, strategies and tactics.

800.2 POLICY

It is the policy of the Madison County Sheriff's Office to utilize crime analysis as a tool in crime control and prevention efforts. This entails gathering, analyzing and correlating data to effectively deploy the resources of this department.

800.3 DATA SOURCES

Crime analysis data is extracted from many sources including, but not limited to:

- Crime reports.
- Parole and probation records.
- Activity records from the Dispatch Center.
- Virginia Criminal Information Network (VCIN).
- Traffic Records Electronic Data System (TREDS).

800.4 CRIME ANALYSIS FACTORS

The following minimum criteria should be used in collecting data for crime analysis:

- Frequency by type of crime
- Geographic factors
- Temporal factors
- Victim and target descriptors
- Suspect descriptors
- Suspect vehicle descriptors
- Modus operandi factors
- Physical evidence information

800.5 CRIME ANALYSIS DISSEMINATION

Information developed through crime analysis should be disseminated to the appropriate divisions or members on a timely basis. Information that is relevant to the operational or tactical plans of specific line members should be sent directly to them. Information relevant to the development of department strategic plans should be provided to the appropriate command staff members.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

When information pertains to tactical and strategic plans, it should be provided to all affected members.

The Madison County Sheriff's Office community liaison should respond to requests for relevant data to crime prevention groups, community regulatory agencies involved with community development and other interested entities. This data should be used to improve community design and construction to mitigate the risk of criminal activity.

800.6 CRIME ANALYSIS APPLICATION

Crime analysis efforts should be aligned with identified public safety needs of the community. Annual assessments should occur to assess the effectiveness of programs and activities targeting public safety and to identify areas for improvement or adjustment.

The Madison County Sheriff's Office community liaison should maintain a relationship with community crime prevention groups and provide two-way discourse for the dissemination of the appropriate crime analysis data and collection of community feedback. Community outreach efforts should integrate all available data with crime analysis techniques to assist the Department in guiding effective community crime prevention group activities.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

The Dispatch Center

801.1 PURPOSE AND SCOPE

This policy establishes guidelines for the basic functions of the Dispatch Center. It addresses the immediate information needs of the Department in the course of its normal daily activities and during emergencies.

801.2 POLICY

It is the policy of the Madison County Sheriff's Office to provide 24-hour telephone service to the public for information and for routine or emergency assistance. The Department provides two-way radio capability for continuous communication between the Dispatch Center and department members in the field.

801.3 THE DISPATCH CENTER SECURITY

The communications function is vital and central to all emergency service operations. The safety and security of the Dispatch Center, its members and its equipment must be a high priority. Special security procedures, including but not limited to the protection of the the Dispatch Center equipment, should be established in a separate operations manual for the Dispatch Center.

Access to the Dispatch Center shall be limited to the Dispatch Center members, the Shift Supervisor, command staff and department members with a specific business-related purpose.

801.4 RESPONSIBILITIES

801.4.1 DISPATCH SUPERVISOR

The Dispatch Supervisor is appointed by and responsible to the Communications/911 Director.

The responsibilities of the Dispatch Supervisor include, but are not limited to:

(a) Overseeing the efficient and effective operation of the Dispatch Center in coordination with other supervisors.

(b) Scheduling and maintaining dispatcher time records.

(c) Supervising, training, and evaluating dispatchers.

(d) Ensuring the radio and telephone recording system is operational.

1. Recordings shall be securely stored and maintained in accordance with the established records retention schedule and as required by law.

(e) Processing requests for copies of the Dispatch Center information for release.

(f) Maintaining the Dispatch Center database systems.

(g) Maintaining and updating the Dispatch Center procedures manual.

1. Procedures for specific types of crime reports may be necessary. For example, specific questions and instructions may be necessary when talking with a victim of a sexual assault to ensure that his/her health and safety needs are met, as well as steps that he/she may take to preserve evidence.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. Procedures for circumstances that require the presence of a supervisor at the scene may be necessary (e.g. notification of a supervisor to request his/her presence at an incident.
3. Ensuring dispatcher compliance with established policies and procedures.

(h) Handling internal and external inquiries regarding services provided and accepting personnel complaints in accordance with the Personnel Complaints Policy.

(i) Maintaining a current contact list of County personnel to be notified in the event of a utility service emergency.

(j) Maintaining a database containing the following information:

1. The name of the deputy in charge.
2. A roster containing the contact telephone number of every sworn agency member.
3. Duty schedule for incoming shifts.
4. Visual maps detailing the Madison County Sheriff's Office's service area.
5. Deputy status information.
6. Written procedures and telephone numbers for procuring emergency and necessary external services to the Madison County Sheriff's Office.

801.4.2 DISPATCHERS

Dispatchers report to the Dispatch Supervisor. The responsibilities of the dispatcher include, but are not limited to:

(a) Receipt and handling of all incoming and transmitted communications, including:

1. Emergency 9-1-1 lines.
2. Business telephone lines.
3. Telecommunications Device for the Deaf (TDD)/Text Telephone (TTY) equipment.
4. Radio communications with department members in the field and support resources (e.g., fire department, emergency medical services (EMS), allied agency law enforcement units).
5. Other electronic sources of information (e.g., text messages, digital photographs, video).

(b) Documenting the field activities of department members and support resources (e.g., fire department, EMS, allied agency law enforcement units).

(c) Inquiry and entry of information through the Dispatch Center, department and other law enforcement database systems (e.g., VCIN, DMV, NCIC).

(d) Monitoring department video surveillance systems.

(e) Maintaining the current status of members in the field, their locations and the nature of calls for service.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(f) Notifying the Shift Supervisor or field supervisor of emergency activity, including, but not limited to:

1. Vehicle pursuits.
2. Foot pursuits.
3. Assignment of emergency response.

801.5 CALL HANDLING

This department provides members of the public with access to the 9-1-1 system for a single emergency telephone number.

When a call for services is received, the dispatcher will reasonably and quickly attempt to determine whether the call is an emergency or non-emergency, and shall quickly ascertain the call type, location and priority by asking four key questions:

- Where?
- What?
- When?
- Who?

If the dispatcher determines that the caller has a hearing and/or speech impairment or disability, he/she shall immediately initiate a connection with the individual via available TDD/TTY equipment or Telephone Relay Service (TRS), as mandated by the Americans with Disabilities Act (ADA).

If the dispatcher determines that the caller is a limited English proficiency (LEP) individual, the dispatcher should quickly determine whether sufficient information can be obtained to initiate an appropriate response. If language assistance is still needed, the language is known and a language-appropriate authorized interpreter is available in the Dispatch Center, the dispatcher should immediately connect the LEP caller to the authorized interpreter.

If no authorized interpreter is available or the dispatcher is unable to identify the caller’s language, the dispatcher will contact the contracted telephonic interpretation service and establish a three-party call connecting the dispatcher, the LEP individual and the interpreter.

Dispatchers should be courteous, patient and respectful when dealing with the public.

801.5.1 EMERGENCY CALLS

A call is considered an emergency when there is an immediate or potential threat to life or serious property damage, and the timely arrival of public safety assistance is of the utmost importance. A person reporting an emergency should not be placed on hold until the dispatcher has obtained all necessary information to ensure the safety of the responding department members and affected individuals.

Emergency calls should be dispatched immediately. The Shift Supervisor shall be notified of pending emergency calls for service when department members are unavailable for dispatch.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

801.5.2 NON-EMERGENCY CALLS
A call is considered a non-emergency call when there is no immediate or potential threat to life or property. A person reporting a non-emergency may be placed on hold, if necessary, to allow the dispatcher to handle a higher priority or emergency call.

The reporting person should be advised if there will be a delay in the dispatcher returning to the telephone line or when there will be a delay in the response for service.

801.6 RADIO COMMUNICATIONS

The sheriff's radio system is for official use only, to be used by dispatchers to communicate with department members in the field. All transmissions shall be professional and made in a calm, businesslike manner, using proper language and correct procedures. Such transmissions shall include, but are not limited to:

(a) Members acknowledging the dispatcher with their radio identification call signs and current location.

(b) Dispatchers acknowledging and responding promptly to all radio transmissions.

(c) Members keeping the dispatcher advised of their status and location.

(d) Member and dispatcher acknowledgements shall be concise and without further comment unless additional information is needed.

The Dispatch Supervisor shall be notified of radio procedure violations or other causes for complaint. All complaints and violations will be investigated and reported to the complainant’s supervisor and processed through the chain of command.

801.6.1 FEDERAL COMMUNICATIONS COMMISSION COMPLIANCE
Madison County Sheriff's Office radio operations shall be conducted in accordance with Federal Communications Commission (FCC) procedures and requirements.

801.6.2 RADIO IDENTIFICATION
Radio call signs are assigned to department members based on factors such as duty assignment, uniformed patrol assignment and/or member identification number. Dispatchers shall identify themselves on the radio with the appropriate station name or number, and identify the department member by his/her call sign. Members should use their call signs when initiating communication with the dispatcher. The use of the call sign allows for a brief pause so that the dispatcher can acknowledge the appropriate department member. Members initiating communication with other law enforcement or support agencies shall use their entire radio call sign, which includes the department station name or number.

801.7 DOCUMENTATION

It shall be the responsibility of the Dispatch Center to document all relevant information on calls for service or self-initiated activity. Dispatchers shall attempt to elicit, document and relay as much information as possible to enhance the safety of the member and assist in anticipating conditions that may be encountered at the scene. Desirable information would include, at a minimum:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

- Incident control number.
- Date and time of request.
- Name and address of the reporting person, if possible.
- Type of incident reported.
- Involvement of weapons, drugs and/or alcohol.
- Location of incident reported.
- Identification of members assigned as primary and backup.
- Time of dispatch.
- Time of the responding member's arrival.
- Time of member's return to service.
- Disposition or status of reported incident.
- A log of the data captured by the computer system, if using a Computer Aided Dispatch (CAD) system.
- Vehicle mileage and transport time when a member is transporting a juvenile or a person of the opposite sex.

All appropriate data will be retained in accordance with an established retention schedule. Data will be purged when it has exceeded the established retention time.

All CAD data will be retained in accordance with an established retention schedule. CAD data will be purged when it has exceeded the established retention time.

801.8 CONFIDENTIALITY

Information that becomes available through the Dispatch Center may be confidential or sensitive in nature. All members of the Dispatch Center shall treat information that becomes known to them as confidential and release that information in accordance with the Protected Information Policy.

Automated data, such as Department of Motor Vehicle records, warrants, criminal history information, records of internal sheriff's files or medical information, shall only be made available to authorized law enforcement personnel. Prior to transmitting confidential information via the radio, an admonishment shall be made that confidential information is about to be broadcast.

801.9 TRAINING AND CERTIFICATION

Members of the Dispatch Center whose duties include dispatching law enforcement personnel and who were hired on or after July 1, 1988, must meet compulsory minimum training standards and shall be certified by the Virginia Department of Criminal Justice Services within 24 months of employment (Va. Code § 9.1-102; 6 VAC 20-60-30).

Members of the Dispatch Center must meet the compulsory minimum training standards for telecommunicator cardiopulmonary resuscitation and emergency medical dispatch developed by the Virginia Department of Health Office of Emergency Medical Services as required by Va. Code

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

§ 56-484.16:1. The Sheriff or authorized designee should provide any necessary equipment for telecommunicator cardiopulmonary resuscitation instruction and establish procedures to maintain the quality of the department’s program as required by Va. Code § 56-484.16:1.

801.10 THE DISPATCH CENTER ALTERNATIVE POWER SOURCE

The Madison County Sheriff's Office shall:

(a) Maintain an alternate electrical power source sufficient for continued operations of emergency communications equipment absent primary power.

(b) Maintain energy resources adequate for 3 days operation of the alternate power source.

(c) Ensure readiness of the alternate source through scheduled routine testing.

(d) Provide and inspect security measures to protect the power source and control/service panels.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Property and Evidence Section

802.1 PURPOSE AND SCOPE

This policy provides guidelines for the proper processing, storage, security and disposition of evidence and other property. This policy also provides for the protection of the chain of custody and identifies those persons authorized to remove and/or destroy property.

802.1.1 DEFINITIONS

Definitions related to this policy include:

Property - All articles placed in secure storage within the Property and Evidence Section, including the following:

- Evidence - Items taken or recovered in the course of an investigation that may be used in the prosecution of a case, including photographs and latent fingerprints.
- Found property - Items found by members of the Department or the public that have no apparent evidentiary value and where the owner cannot be readily identified or contacted.
- Safekeeping - Items received by the Department for safekeeping, such as a firearm, the personal property of an arrestee that has been not taken as evidence and items taken for safekeeping under authority of law.
- **Unclaimed property** - Any personal property belonging to another which has been acquired by a law-enforcement officer pursuant to his duties, which is not needed in any criminal prosecution, which has not been claimed by its rightful owner and which the State Treasurer has indicated will be declined if remitted under the Virginia Disposition of Unclaimed Property Act (§ 55.1-2500 et seq.) (Va. Code §15.2-1719).

802.2 POLICY

It is the policy of the Madison County Sheriff's Office to process and store all property in a manner that will protect it from loss, damage or contamination, while maintaining documentation that tracks the chain of custody, the location of property and its disposition.

802.3 PROPERTY AND EVIDENCE SECTION SECURITY

The Property and Evidence Section shall maintain secure storage and control of all property in the custody of this department. A evidence technician shall be appointed by and will be directly responsible to the Sheriff or the authorized designee. The evidence technician is responsible for the security of the Property and Evidence Section.

802.3.1 REFUSAL OF PROPERTY

The evidence technician has the obligation to refuse any piece of property that is hazardous or that has not been properly documented or packaged. Should the evidence technician refuse an item of property, he/she shall maintain secure custody of the item in a temporary property locker or other safe location and inform the submitting member's supervisor of the reason for refusal and the action required for acceptance into the Property and Evidence Section.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

802.3.2 KEY CONTROL

Property and Evidence Section keys should be maintained by the evidence technician and members assigned to the Property and Evidence Section. An additional set of keys should be kept in a sealed and initialed envelope in an after-hours key box. Property and Evidence Section keys shall not be loaned to anyone and shall be maintained in a secure manner. If a Property and Evidence Section key is lost, all access points shall be re-keyed and new keys issued as necessary. After-hours access to the Property and Evidence Section via the additional set of keys must be documented in a memorandum and submitted to the Investigation Division Supervisor as soon as practicable.

Only authorized members shall have limited access to secure property storage areas when the Property and Evidence Section is closed.

802.3.3 ACCESS

Only authorized members assigned to the Property and Evidence Section shall have access to property storage areas. Any individual who needs to enter a property storage area (e.g., maintenance or repair contractors) must be approved by the Investigation Division Supervisor and accompanied by the evidence technician. Each individual must sign the Property and Evidence Section access log and indicate:

(a) The date and time of entry and exit.

(b) The purpose for access, including the specific case or property number.

Each access log entry shall be initialed by the accompanying department member.

Only authorized members shall have limited access to secure property storage areas when the Property and Evidence Section is closed.

802.3.4 SECURE STORAGE

All property in the custody of the Department, both evidentiary and non-evidentiary, shall be stored within designated, secure areas. The Department shall provide secure facilities for the storage of property in the Department's custody during periods when the Property and Evidence Section is closed.

802.4 PROPERTY HANDLING

The member who first comes into possession of any property is generally responsible for the care, custody and control of such property until it is transferred to the evidence technician and/or processed and placed in a temporary property locker or storage area. Care shall be taken to maintain the chain of custody for all items of evidence.

Whenever property is taken from an individual, a property receipt form will be completed. The receipt shall describe the property and contain a notice on how to retrieve the property from the Department. A copy of the property receipt form shall be given to the individual from whom the property was taken.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Property and Evidence Section

802.4.1 PROCESSING AND PACKAGING

All property must be processed by the responsible member prior to the member going off-duty, unless otherwise approved by a supervisor. Members shall process and package property as follows:

(a) A property form shall be completed describing each item. List all known information, including:

1. Serial number.
2. Owner's name.
3. Finder's name.
4. Other identifying information or marking.

(b) Each item shall be marked with the member's initials and the date processed using a method that will not damage, deface, degrade, or devalue the item. Items too small or too delicate to mark should be individually packaged and labeled and the package marked with the member's initials and date.

(c) Property shall be packaged in a container suitable for its size.

(d) A property tag shall be completed and attached to the property or container in which the property is stored.

(e) The case number shall be indicated on the property tag and the container.

(f) The property form, without the hard card portion (property control card), shall be submitted with the case report.

(g) The case report shall describe each item of property obtained and detail the circumstances by which the property came into the Department's possession.

(h) The property control card shall be submitted with the property directly to the evidence technician or placed in a temporary property locker. Items too large to fit in a temporary property locker may be placed in a designated storage area that can be secured from unauthorized entry, and the property control card placed in a temporary property locker.

802.4.2 EXCEPTIONAL PROCESSING

The following items require special consideration and shall be processed as follows, unless special conditions dictate a reasonable deviation:

Bicycles - Bicycles and bicycle frames shall have a property tag securely attached and should be placed in the bicycle storage area.

Biological and related items - Evidence that may contain biological samples shall be indicated as such on the property form.

Property stained with bodily fluids, such as blood or semen, shall be air-dried in a secure location (e.g., locked drying cabinet) prior to processing.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Property and Evidence Section

Items of evidence collected from a crime scene that require specific storage requirements pursuant to laboratory processing shall have such storage requirements clearly indicated on the property form.

Items that are potential biohazards shall be appropriately packaged and marked "Biohazard" to reduce the risk of exposure or contamination.

Cash - Cash shall be counted in the presence of another member. The cash shall be placed in a property envelope and initialed by both members. A supervisor shall be contacted for cash in excess of $1,000. The supervisor shall witness the count, initial and date the envelope, and specify any additional security procedures that may be necessary.

Explosives and fireworks - Explosives will not be retained in the sheriff's facility. Fireworks that are considered stable and safe, as well as road flares or similar signaling devices, may be stored in proper containers in an area designated for storage of flammable materials.

The evidence technician is responsible for transporting to the fire department, on a regular basis, any fireworks or signaling devices that are not retained as evidence.

Firearms and other weapons - Firearms shall be unloaded and packaged separately from ammunition. Knife boxes should be used to package knives. Receipts should be provided for firearms surrendered by persons subject to protective orders as provided by Va. Code § 18.2-308.1:4.

Government property - License plates that have not been reported stolen or are of no evidentiary value should be placed in the designated container for return to the Department of Motor Vehicles. No formal property processing is required.

County property that is of no evidentiary value should be released directly to the appropriate County department. No formal property processing is required.

If no responsible County personnel can be located, the property should be held for safekeeping.

Jewelry, gemstones, and precious metals - Jewelry, gemstones, and precious metals shall be inventoried in the presence of another member. The items shall be packaged, sealed, and initialed by both members. A supervisor shall be contacted for value in excess of $500. The supervisor shall witness the inventory, initial, and date the package, and specify any additional security procedures that may be necessary.

Sharps - Syringe tubes should be used to package syringes and needles.

802.4.3 CONTROLLED SUBSTANCES AND DANGEROUS DRUGS

(a) Controlled substances and dangerous drugs shall not be packaged with other property, but shall be processed separately using a separate property form.

(b) The member processing controlled substances and dangerous drugs shall retain such property in his/her possession until it is weighed, packaged, tagged and placed in the

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

designated controlled substances and dangerous drugs locker, accompanied by the property control card and lab copy of the property form.

(c) Prior to packaging and if the quantity allows, a presumptive test should be made on all suspected controlled substances. If conducted, the result of the test shall be included in the crime report.

1. The member shall package controlled substances and dangerous drugs as follows:

(a) Maintain the property in the container in which it was seized and place it in a property envelope of appropriate size.

(b) Seal and initial the property envelope and cover the initials with cellophane tape.

(c) Weigh the property envelope to obtain the Gross Package Weight (GPW).

(d) Write the GPW and then initial and date both the outside of the package and the property form.

(d) When the quantity of controlled substances and dangerous drugs exceeds the available safe storage capacity as determined by the evidence technician, the quantity shall be photographed and weighed.

1. A representative sample of sufficient quantity to allow scientific analysis of the controlled substances and dangerous drugs should be taken as allowed by state law and placed in a separate package or container.

2. Excess quantities should be stored or disposed of as required by law or directed by court order.

(e) Marijuana with any perceptible moisture content shall be loosely packaged in a container that allows for drying or shall be dried prior to storage. The evidence technician shall monitor stored marijuana for growth of mold.

802.5 RECORDING OF PROPERTY

The evidence technician receiving custody of property shall ensure a property control card for each item or group of items is created. The property control card will be the permanent record of the property in the Property and Evidence Section. The evidence technician will record on the property control card his/her signature, GPW if the package contains controlled substances/narcotics and dangerous drugs, the date and time the property was received and where the property will be stored.

A unique property number shall be obtained for each item or group of items from the property log. This number shall be recorded on the property form, property tag and the property control card. The property log shall document the following:

(a) Property number

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Case number

(c) Property tag number

(d) Item description

(e) Item storage location

(f) Receipt, release and disposal dates

Any change in the location of property held by the Madison County Sheriff's Office shall be noted in the property log.

802.6 PROPERTY CONTROL

The evidence technician temporarily relinquishing custody of property to another person shall record on the property control card his/her signature, the date and time the property was released, the name and signature of the person accepting custody of the property and the reason for release.

Any member receiving property shall be responsible for such property until it is returned to the Property and Evidence Section or released to another authorized person or entity.

The return of the property to the Property and Evidence Section should be recorded on the property control card, indicating the date, the time, the name and the signature of the person who returned the property and the name and signature of the person to whom the property was returned.

The property and evidence should be entered into the appropriate databases for automated and electronic searching and identification.

802.6.1 EVIDENCE

Every time evidence is released or received, an appropriate entry on the property control card shall be completed to maintain the chain of custody. No evidence is to be released without first receiving written authorization from the Investigation Division supervisor or investigator.

The temporary release of evidence to members for investigative purposes or for court proceedings shall be noted on the property control card, stating the date, time and to whom it was released. Requests for items of evidence needed for court proceedings shall be submitted to the evidence technician at least one day prior to the court date.

Requests for laboratory analysis shall be completed on the appropriate lab form and submitted to the evidence technician. This request may be submitted any time after the property has been processed.

802.6.2 TRANSFER OF EVIDENCE TO CRIME LABORATORY

The evidence technician releasing items of evidence for laboratory analysis must complete the required information on the property control card. The transporting member will acknowledge receipt of the evidence by indicating the date and time on the property control card. The lab form will be transported with the evidence to the examining laboratory. Upon delivering the item, the member will record the delivery time on the lab form and the property control card, and obtain

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

the signature of the person accepting responsibility for the evidence. The original copy of the lab form will remain with the evidence and a copy of the form will be returned to the Records Division for filing with the case.

802.6.3 CONTROLLED SUBSTANCES AND DANGEROUS DRUGS
The Investigation Division will be responsible for the storage, control and destruction of all controlled substances and dangerous drugs coming into the custody of this department. The GPW will be verified every time controlled substances and dangerous drugs are checked in or out of the Property and Evidence Section and any discrepancies noted on the outside of the package. Any change in weight should be immediately reported to the Investigation Division Supervisor.

802.6.4 UNCLAIMED MONEY
The evidence technician shall submit an annual report, or more frequently as directed, regarding money that is presumed to have been abandoned to the Sheriff and the County department responsible for auditing property. The evidence technician may deposit such money in compliance with existing laws upon receipt of proper authorization from the Sheriff (Va. Code § 55.1-2500 et seq.).

802.7 RELEASE OF PROPERTY

The Investigation Division shall authorize the release of all property coming into the care and custody of the Department.

Release of property shall be made upon receipt of an authorized property release form, listing the name and address of the person to whom the property is to be released. The property release form shall be signed by the authorizing supervisor or investigator, and must conform to the items listed on the property control card or must specify the specific items to be released. Release of all property shall be documented on the property control card.

All reasonable attempts shall be made to identify both the rightful owner of found property and items held for safekeeping, and all required notices shall be given (Va. Code § 15.2-1719).

Found property and property held for safekeeping shall be retained for the period of time required by law. During such period, Property and Evidence Section members shall attempt to contact the rightful owner by telephone and/or mail when sufficient identifying information is available. The final disposition of all such property shall be fully documented on the property control card.

A evidence technician shall release such property when the owner presents proper identification and an authorized property release form has been received. The signature of the person receiving the property shall be recorded on the property control card.

If any item listed on a property control card has not been released, the property control card will remain with the Property and Evidence Section. When all property listed on the card has been released, the card shall be forwarded to the Records Division for filing with the case, and the release of all items shall be documented in the property log.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

802.7.1 DISCREPANCIES
The Shift Supervisor shall be notified whenever a person alleges that there is a shortage or discrepancy regarding his/her property. The Shift Supervisor will interview the person claiming the shortage. The Shift Supervisor shall ensure that a search for the alleged missing items is completed and shall attempt to prove or disprove the claim.

802.7.2 DISPUTED CLAIMS TO PROPERTY
Occasionally, more than one party may claim an interest in property being held by this department, and the legal rights of the parties cannot be clearly established. Such property shall not be released until one party has obtained a valid court order or establishes an undisputed right to the property.

All parties should be advised that their claims are civil. In extreme situations, legal counsel for this department should be contacted.

802.7.3 RELEASE OF FIREARMS
Firearms or ammunition should be released within any time periods provided by law and should only be released upon presentation of valid identification and authorized documents showing that the individual may legally possess the item (Va. Code § 18.2-308.1:4; Va. Code § 19.2-152.15; Va. Code § 52-25.1).

802.8 DESTRUCTION OR DISPOSAL OF PROPERTY
An authorized Investigation Division investigator or supervisor shall approve the destruction or disposal of all property held by this department.

All property not held for evidence in a pending criminal investigation or proceeding may be destroyed or disposed of in compliance with existing laws upon reasonable notice to the owner at their last known address of record or, if unknown, by publication and receipt of proper authorization from a supervisor. The disposition of all property shall be entered on the property control card and property log. The final disposition of property or evidence should be completed within six months after legal requirements have been satisfied or completed.

The following types of property shall be destroyed or disposed of in the manner and at the time prescribed by law, unless a different disposition is ordered by a court:

- Weapons or devices declared by law to be illegal to possess
- Unclaimed or surrendered firearms or other weapons (Va. Code § 15.2-1721; Va. Code § 18.2-308.1:4; Va. Code § 19.2-152.15)
- Controlled substances or dangerous drugs declared by law to be illegal to possess without a legal prescription (Va. Code § 19.2-386.23)
- Seized property from illegal transactions (Va. Code § 19.2-386.15 et seq.)
- Unclaimed property (except firearms) (Va. Code § 15.2-1719)
- Bicycles, mopeds and electric personal assistive mobility devices (Va. Code § 15.2-1720).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Property and Evidence Section

802.8.1 BIOLOGICAL EVIDENCE

The evidence technician shall ensure that no biological evidence held by this department is destroyed without adequate notification to the following persons, when applicable (Va. Code § 19.2-11.8):

(a) The defendant

(b) The defendant’s attorney

(c) The appropriate prosecutor and Attorney General

(d) Any sexual assault victim

(e) The Investigation Division Supervisor

(f) The applicable court

Biological evidence shall be retained for a minimum period established by law or the expiration of any sentence imposed related to the evidence, whichever time period is greater (Va. Code § 19.2-11.8). Following the retention period, notifications should be made by certified mail and should inform the recipient that the evidence will be destroyed after a date specified in the notice, unless a motion seeking an order to retain the sample is filed and served on this department within 90 days of the date of the notification. A record of all certified mail receipts shall be retained in the appropriate file. Any objection to, or motion regarding, the destruction of the biological evidence should be retained in the appropriate file and a copy forwarded to the Investigation Division Supervisor.

Biological evidence related to a homicide shall be retained indefinitely and may only be destroyed with the written approval of the Sheriff and the head of the applicable prosecutor’s office.

Biological evidence from an unsolved sexual assault should not be disposed of prior to expiration of the statute of limitations. Even after expiration of the applicable statute of limitations, the Investigation Division Supervisor should be consulted and the sexual assault victim should be notified.

802.8.2 VICTIM OBJECTION

If a sexual assault victim makes a written objection to the destruction of biological evidence, the evidence shall be retained for a period of 10 years after receipt of the objection. Upon the expiration of this 10-year period, the victim should be notified prior to the destruction of the evidence unless the victim has made a written request not to be contacted for this purpose. Once the victim has been notified, the evidence may be destroyed if the victim does not respond within the time period designated in this policy or if the victim consents to the destruction (Va. Code § 19.2-11.8).

802.8.3 MARIJUANA

At the first sign of mold growth, stored marijuana shall be photographed showing the mold growth. As soon as practicable, the evidence technician shall make efforts to lawfully destroy the contaminated marijuana, in compliance with this policy. The evidence technician should consult with the member assigned to the case investigation for authorization to destroy the

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

remaining marijuana, after taking representative samples, and should request assistance from the appropriate prosecutor in obtaining a court order for immediate destruction.

802.8.4 MEDICAL MARIJUANA

The investigating member should advise the evidence technician and the prosecutor if the party from whom the marijuana was seized holds a valid medical permit to possess marijuana or claims that the possession of the marijuana is for medical purposes (Va. Code § 18.2-251.1).

The evidence technician shall store marijuana, drug paraphernalia or other related property that is seized from a person engaged in or assisting with the use of medical marijuana in a manner that is consistent with the provisions of the Medical Marijuana Policy.

Marijuana that is infected with mold shall not be returned. This includes marijuana seized from a person who holds a valid medical permit to possess marijuana or who claims that possession of the marijuana is for medical purposes.

802.9 INSPECTION OF THE PROPERTY AND EVIDENCE SECTION

The Property and Evidence Section shall conduct quarterly documented inspections to ensure the adherence to applicable policies and procedures.

The Investigation Division Supervisor shall ensure that periodic, unannounced inspections of the Property and Evidence Section operations and storage facilities are conducted at least twice a year to ensure adherence to appropriate policies and procedures. The Investigation Division Supervisor also shall ensure that an audit is conducted annually, or as directed by the Sheriff. Inspections and audits shall be conducted by a member of this department who is not routinely or directly connected with the Property and Evidence Section operations.

Whenever there is a change of assignment for any member with authorized access to the Property and Evidence Section, an inventory of all property shall be conducted by a person who is not associated with the Property and Evidence Section or its function. This is to ensure that all property is accounted for and the records are correct.

Whenever the primary manager assigned to the Property and Evidence Section is reassigned, the new manager and a designee of the Sheriff shall conduct a joint inspection to ensure all property is accounted for and records in proper order.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Records Division

803.1 PURPOSE AND SCOPE

This policy establishes the guidelines for the operational functions of the Madison County Sheriff's Office Records Division. The policy addresses department file access and internal requests for case reports.

803.2 POLICY

It is the policy of the Madison County Sheriff's Office to maintain department records securely, professionally and efficiently (Va. Code § 15.2-1722).

803.3 RESPONSIBILITIES

803.3.1 RECORDS MANAGER

The Sheriff shall appoint and delegate certain responsibilities to a Records Manager. The Records Manager shall be directly responsible to the Administration Division Supervisor or the authorized designee.

The responsibilities of the Records Manager include, but are not limited to:

(a) Overseeing the efficient and effective operation of the Records Division.

(b) Scheduling and maintaining Records Division time records.

(c) Supervising, training and evaluating Records Division staff.

(d) Maintaining and updating a Records Division procedure manual.

(e) Ensuring compliance with established policies and procedures.

(f) Supervising the access, use and release of protected information (see the Protected Information Policy).

(g) Establishing security and access protocols for case reports designated as sensitive, where additional restrictions to access have been implemented. Sensitive reports may include, but are not limited to:

1. Homicides
2. Cases involving department members or public officials
3. Any case where restricted access is prudent

803.3.2 RECORDS DIVISION

The responsibilities of the Records Division include, but are not limited to:

(a) Maintaining a records management system for case reports.

1. The records management system should include a process for numbering, identifying, tracking and retrieving case reports.

(a) A process for numbering, identifying, tracking and retrieving case reports.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) An alphabetical master name index, physical or electronic, to serve as a cross reference to all documents in which a person has been named.

(c) A process for documenting incident by type of offense or report, incidents by location, stolen property and recovered property.

(d) A case file management system for criminal investigations to include case status, assigned coordinator, types of records, and authorized access.

(b) Entering case report information into the records management system.

1. Modification of case reports shall only be made when authorized by a supervisor.

(c) Providing members of the Department with access to case reports, physical or electronic, 24 hours a day.

(d) Maintaining compliance with federal, state and local regulations regarding reporting requirements of crime statistics.

(e) Maintaining compliance with federal, state and local regulations regarding criminal history reports and auditing.

(f) Identifying missing case reports and notifying the responsible member’s supervisor.

(g) Preparing and maintaining an annual report of the department's activities and statistical data summaries.

803.4 FILE ACCESS AND SECURITY

The security of files in the Records Division must be a high priority and shall be maintained as mandated by state or federal law. All case reports including, but not limited to, initial, supplemental, follow-up, evidence and any other reports related to a sheriff's department case, including field interview (FI) cards, criminal history records and publicly accessible logs, shall be maintained in a secure area within the Records Division, accessible only by authorized members of the Records Division. Access to case reports or files when Records Division staff is not available may be obtained through the Shift Supervisor.

The Records Division will also maintain a secure file for case reports deemed by the Sheriff as sensitive or otherwise requiring extraordinary access restrictions. Records or reports relating to active vice, drug and organized crime investigations shall be maintained in a secure manner separate from the central records system. The Records Manager will ensure that procedures are in place for the separation of juvenile criminal arrest records from adult criminal arrest records pursuant to Virginia law.

803.4.1 ORIGINAL CASE REPORTS

Generally, original case reports shall not be removed from the Records Division. Should an original case report be needed for any reason, the requesting department member shall first obtain authorization from the Records Manager. All original case reports removed from the Records Division shall be recorded on a designated report check-out log, which shall be the only authorized manner by which an original case report may be removed from the Records Division.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Records Division

All original case reports to be removed from the Records Division shall be photocopied and the photocopy retained in the file location of the original case report until the original is returned to the Records Division. The photocopied report shall be shredded upon return of the original report to the file.

803.4.2 WARRANT FILES

Management of warrant files should be performed by the Records Division.

(a) Warrant files maintenance procedure:

1. Warrant files should be stored in a secure file cabinet accessible only by authorized staff.
2. Warrant files should be cross referenced with the Master Name index.
3. Access to warrant files should be available 24 hours a day/ 7 days a week by members tasked with warrant verification/validation.
4. Warrant files should contain at least one original copy of the warrant bearing the seal of the court of jurisdiction and signature of the issuing judge or magistrate. In addition the warrant should have:
    (a) The name, description, and known identifying information of the wanted person.
    (b) The date of issue.
    (c) The case number.
    (d) An attached document guaranteeing extradition up to the set limits and identifying the authorizing person.
    (e) A separate location for the storage of served or quashed warrants pending return to the court of origination.
5. All warrants that have been confirmed served or quashed should be removed from the external information systems in which they were entered.
    (a) The subject's name should be run through all systems after the removal to verify that original entry has been removed or canceled.
    (b) A red sheet or other marking instrument indicating the warrant has been served or quashed with the service information (e.g., date, time, location, agency) should be attached to the warrant.
6. A copy of the National Crime Information Center (NCIC) system, National Law Enforcement Telecommunications System (NLETS) or the Virginia Criminal Information Network (VCIN) confirmation of the warrant and a copy of the fax receipt should be attached to the warrant.
7. All warrant entries, removals, and transmissions in external information systems should be conducted in compliance with NCIC, NLETS, and VCIN rules and protocols.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

8. Warrant files should be audited annually for out of date or quashed warrants, warrants missing essential information, or extradition guarantee.

(b) Warrant confirmation occurs when a law enforcement officer on the scene with the person suspected to be the wanted subject has received and matched all of the identifying information from the warrant file with the suspect.

(c) Warrant service requires:

1. Resolution of any discrepancies in identifying information is the responsibility and at the discretion of the law enforcement officer on the scene.

2. Service is completed upon the arrest of the wanted subject.

803.5 CONFIDENTIALITY

Records Division staff has access to information that may be confidential or sensitive in nature. Records Division staff shall not access, view or distribute, or allow anyone else to access, view or distribute any record, file or report, whether in hard copy or electronic file format, or any other confidential, protected or sensitive information except in accordance with the Records Maintenance and Release and Protected Information policies and the Records Division procedure manual.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Records Maintenance and Release

804.1 PURPOSE AND SCOPE

This policy provides guidance on the maintenance and release of department records. Protected information is separately covered in the Protected Information Policy.

804.2 POLICY

The Madison County Sheriff's Office is committed to providing public access to records in a manner that is consistent with the Virginia Freedom of Information Act (FOIA) (Va. Code § 2.2-3700 et seq.).

804.3 CUSTODIAN OF RECORDS

The Sheriff shall designate a Custodian of Records (Va. Code § 2.2-3704.2). The responsibilities of the Custodian of Records include but are not limited to:

(a) Managing the records management system for the Department, including the retention, archiving, release, and destruction of department public records.

(b) Maintaining, updating, and complying with the department records retention schedule, including:

1. Identifying the minimum length of time the Department must keep records.
2. Identifying the department division responsible for the original record.

(c) Establishing rules regarding the inspection and copying of department public records as reasonably necessary for the protection of such records.

(d) Identifying records or portions of records that are confidential under state or federal law and not open for inspection or copying.

(e) Establishing rules regarding the processing of subpoenas for the production of records.

(f) Ensuring the availability of a current schedule of fees for public records as allowed by law (Va. Code § 2.2-3704).

(g) Preparing and ensuring the following information is made available to the public upon request and posted on the department website, as required by Va. Code § 2.2-3704.1:

1. In plain English, a description of the basic rights of a person who requests public information, the responsibilities of the Department and the procedures, to include the cost of inspecting or obtaining copies
2. Contact information for the Custodian of Records
3. A general description, summary, list, or index of the types of public records maintained by this department and exemptions in law that permit or require such records to be withheld from release
4. The policy concerning the type of public records the Department routinely withholds from release as permitted by law

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

5. The following statement: "A public body may make reasonable charges not to exceed its actual cost incurred in accessing, duplicating, supplying, or searching for the requested records and shall make all reasonable efforts to supply the requested records at the lowest possible cost. No public body shall impose any extraneous, intermediary, or surplus fees or expenses to recoup the general costs associated with creating or maintaining records or transacting the general business of the public body. Any duplicating fee charged by a public body shall not exceed the actual cost of duplication. Prior to conducting a search for records, the public body shall notify the requester in writing that the public body may make reasonable charges not to exceed its actual cost incurred in accessing, duplicating, supplying, or searching for requested records and inquire of the requester whether he would like to request a cost estimate in advance of the supplying of the requested records as set forth in subsection F of § 2.2-3704 of the Code of Virginia."
6. A written description of how the Department assesses charges for accessing and searching for requested records, and the current associated charges, if any.

(h) Acting as the department's FOIA officer, designating additional members as FOIA officers to receive requests from the public, and ensuring updated contact information for the Records Custodian and any additional FOIA officers is maintained on the department's website or otherwise made easily available to the public as required by Va. Code § 2.2-3704.2.

(i) Confirming that the online posting requirement relating to the Freedom of Information Advisory Council's comment form has been complied with as required by Va. Code § 2.2-3704.1.

804.4 PROCESSING REQUESTS FOR PUBLIC RECORDS

Any department member who receives a request for any record shall forward the request to the Sheriff's Administrative Assistant who shall route the request to the proper officer for review and compliance.

804.4.1 REQUESTS FOR RECORDS

The processing of requests for any record is subject to the following (Va. Code § 2.2-3704):

(a) A request for records should be in writing, identify the requested records with reasonable specificity, and include the name of the requester and the requester's legal address.

(b) The Department is not required to create records that do not exist.

(c) Prior to making a search for requested records, the Department should notify the requester in writing that reasonable charges not to exceed actual costs may be assessed and ask whether a cost estimate is desired in advance.

(d) A request for records shall be responded to promptly but in all cases within five working days of receiving the request. Failure to respond to a request shall be deemed a denial and a violation of FOIA. A request shall be responded to with one of the following:

1. Provide the requested records to the requester.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. If the records are not provided, supply a written response that the requested records are being withheld as exempted by law. The response shall identify the volume and subject matter of the withheld records and include the citation to the specific Code of Virginia statute authorizing the records to be withheld.

3. If the records are provided in part, supply a written response that the requested records are being provided in part and being withheld in part as prohibited by law. The response shall identify the subject matter of the withheld portions and citation to the specific Code of Virginia statute authorizing the records to be withheld. When a record contains material with release restrictions and material that is not subject to release restrictions, the restricted material shall be redacted and the unrestricted material released (Va. Code § 2.2-3704.01).

    (a) A copy of the redacted release should be maintained in the case file for proof of what was actually released and as a place to document the reasons for the redactions. If the record is audio or video, a copy of the redacted audio/video release should be maintained in the department-approved media storage system and a notation should be made in the case file to document the release and the reasons for the redacted portions.

4. If the records cannot be found or do not exist, supply a written response explaining this. However, if it is known that another public body has the requested records, the response shall include the contact information for the other public body.

5. If the records cannot be provided within five working days, supply a written response that it is not practically possible to provide the requested records or to determine whether they are available within the five-workday period. The response shall specify the conditions that make the request impossible. If this response is made within five working days, the Department shall have an additional seven working days, or 60 working days in the case of a request for criminal investigative files under Va. Code § 2.2-3706.1, to provide the requester with a written response to the original request.

    (a) Records that contain criminal investigative files related to a criminal investigation or proceeding are governed by Va. Code § 2.2-3706.1, which requires victim notification under certain circumstances and provides for when disclosure is mandatory, permissive, or prohibited. Response periods are tolled under certain circumstances when a victim seeks an injunction from disclosure.

    (b) If additional time is required to respond to a request because the request is for an extraordinary volume of records or an extraordinarily lengthy search is required, the Custodian of Records shall contact the requester to reach an agreement concerning additional time in which to respond to the request. If an agreement is not reached, legal counsel for the Department should be contacted for filing a petition to the appropriate court to obtain additional time to respond to the request.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(e) The period for providing records is tolled for the amount of time that elapses between notice of the cost estimate and the response of the requester. If the Department receives no response from the requester within 30 days of sending the cost estimate, the request may be considered withdrawn.

(f) The time for providing records may also be tolled if the Department determines that the cost of producing the records will exceed $200 and requests a deposit from the person requesting the records as allowed by law.

(g) Nonexempt records maintained in an electronic database shall be produced in any tangible medium identified by the requester, if that medium is used by this department in the regular course of business.

804.4.2 REQUESTS FOR SENSITIVE SECURITY INFORMATION

If a request is received seeking information relating to the prevention or response to terrorist activity or cyberattacks (including information about infrastructure security plans and systems), and the release of the information might jeopardize the safety of any person or reveal the location of security or other sensitive systems or equipment, the Custodian of Records shall notify the Secretary of Public Safety and Homeland Security of the request and the department's response to the request (Va. Code § 2.2-3705.2).

804.4.3 MANDATORY RELEASE

When requested, records of completed suicide, accidental and natural death investigations where no criminal charges will be initiated shall be released to the parent or spouse of the decedent or, if there is no living parent or spouse, to the most immediate family member of the decedent, provided the person is not a person of interest or a suspect (Va. Code § 2.2-3706).

804.5 RELEASE RESTRICTIONS

Examples of release restrictions include:

(a) Personal identifying information, including an individual's photograph; Social Security and driver's license identification numbers; name, address, and telephone number; and medical or disability information that is contained in any driver's license record, motor vehicle record, or any department record, including traffic accident reports, are restricted except as authorized by the Department, and only when such use or disclosure is permitted or required by law to carry out a legitimate law enforcement purpose (18 USC § 2721; 18 USC § 2722).

(b) Personnel records containing information concerning identifiable members (Va. Code § 2.2-3705.1).

(c) Records that would disclose a member's telephone numbers for cellular telephones, pagers, or comparable portable communication devices provided to members for use in the performance of their official duties (Va. Code § 2.2-3706).

(d) Personal information as defined in Va. Code § 2.2-3801, including but not limited to a driver's license number, Social Security number, agency-issued identification number, education, and medical history.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(e) Personal contact information, as defined in Va. Code § 2.2-3705.1, furnished to the Department for the purpose of receiving electronic mail from this department provided the recipient has requested the non-disclosure.

(f) Records that contain information related to undercover operations or protective details that would reveal the staffing, logistics, or tactical plans of such undercover operations or protective details (Va. Code § 2.2-3706).

(g) Background investigation records of law enforcement employment applicants for law enforcement employment, administrative investigations relating to allegations of wrongdoing by members, and other administrative investigations conducted by the Department that are made confidential by law (Va. Code § 2.2-3706).

(h) The identity of any individual providing information about a crime or criminal activity under a promise of anonymity (Va. Code § 2.2-3706).

(i) Victim or witness information as provided in Va. Code § 19.2-11.2, as well as certain photographic, audio, video, and other information as provided in Va. Code § 2.2-3706.1.

(j) Juvenile law enforcement records, except for those authorized to receive such information as provided in Va. Code § 16.1-301 and Va. Code § 16.1-309.

(k) Criminal investigation files including complaints, court orders, notes, memoranda, diagrams, maps, photographs, correspondence, reports, witness statements, and evidence relating to a criminal investigation or prosecution not required to be disclosed in accordance with Va. Code § 2.2-3706.1 (Va. Code § 2.2-3706).

(l) Portions of noncriminal incident or other noncriminal investigative reports or materials that contain identifying information of a personal, medical, or financial nature where the release of such information would jeopardize the safety or privacy of any person (Va. Code § 2.2-3706).

(m) Records relating to neighborhood watch programs (Va. Code § 2.2-3706).

(n) Confidential records, including victim identities provided to staff of a rape crisis center or a program for battered spouses (Va. Code § 2.2-3705.2).

(o) Documentation or other information that describes the design, function, operation, or access control features of any department security system used to control access to or use of any automated data processing or telecommunications systems, including the Statewide Agencies Radio System (STARS) (Va. Code § 2.2-3705.2).

(p) Plans and information to prevent or respond to terrorist activity or cyberattacks, the disclosure of which would jeopardize the safety of any person (Va. Code § 2.2-3705.2).

(q) Records that contain specific tactical plans, the disclosure of which would jeopardize the safety or security of law enforcement personnel or the general public (Va. Code § 2.2-3706).

(r) Any other information that may be appropriately denied by Virginia law.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

804.6 SUBPOENAS AND DISCOVERY REQUESTS

Any member who receives a subpoena duces tecum or discovery request for records should promptly contact a supervisor and the Custodian of Records for review and processing. While a subpoena duces tecum may ultimately be subject to compliance, it is not an order from the court that will automatically require the release of the requested information.

Generally, discovery requests and subpoenas from criminal defendants and their authorized representatives (including attorneys) should be referred to the Commonwealth Attorney, County Attorney or the courts.

All questions regarding compliance with any subpoena duces tecum or discovery request should be promptly referred to legal counsel for the Department so that a timely response can be prepared.

804.7 RELEASED RECORDS TO BE MARKED

Each page of any written record released pursuant to this policy should be stamped in a colored ink or otherwise marked to indicate the department name and to whom the record was released.

Each audio/video recording released shall include the department name and to whom the record was released.

804.8 SECURITY BREACHES

Members who become aware that any Madison County Sheriff's Office system containing personal information may have been breached should notify the Sheriff as soon as practicable.

The Sheriff shall ensure the required notice is given to any resident of this state whose unsecured personal information is reasonably believed to have been acquired by an unauthorized person (Va. Code § 18.2-186.6). Notice shall also be provided to the Office of the Attorney General. Notice shall be in the form and manner specified in Va. Code § 18.2-186.6.

Notice shall be given as soon as reasonably practicable and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system. Notice may be delayed if notification will impede a criminal or civil investigation or homeland or national security (Va. Code § 18.2-186.6).

If notification is required to more than 1000 persons at one time, notice of the timing, distribution, and content of notices sent as a result of the breach shall be provided to the Office of the Attorney General and all consumer reporting agencies as specified in Va. Code § 18.2-186.6.

For the purposes of the notice requirement, personal information includes an individual's first name or first initial and last name in combination with, and linked to, any one or more of the following:

(a) Social Security number

(b) Driver's license number or Virginia identification card number

(c) Full account number, credit, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial accounts

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Passport number

(e) Military identification number

If the breach reasonably appears to have been made to protected information covered in the Protected Information Policy, the Sheriff/Administrative Assistant should promptly notify the appropriate member designated to oversee the security of protected information (see the Protected Information Policy).

804.8.1 BREACH OF TAXPAYER IDENTIFICATION DATA

In the event that both the taxpayer identification number of any department member and the amount of income tax withheld for that member are breached, the Records Manager shall notify the Office of the Attorney General in accordance with Va. Code § 18.2-186.6(M).

804.9 EXPUNGEMENT AND SEALING

Expungement orders received by the Department shall be reviewed for appropriate action by the Custodian of Records. The Custodian of Records shall expunge such records as ordered by the court. Records may include but are not limited to a record of arrest, investigation, detention, or conviction. Once a record is expunged, members shall respond to any inquiry as though the record did not exist (Va. Code § 19.2-392.2).

Sealing orders received by the Department shall also be reviewed for appropriate action by the Custodian of Records. Records may include those related to arrests, charges, and convictions. Once a record is ordered sealed, members shall respond to any inquiry as though the record did not exist unless otherwise permitted or required by law (Va. Code § 19.2-392.5 et seq.).

804.10 TRAINING

The Training Supervisor should establish procedures for the Custodian of Records and any additional FOIA officers to receive training on Virginia’s FOIA statute from the department’s legal counsel or the Virginia Freedom of Information Advisory Council as required by Va. Code § 2.2-3704.2. The procedures should include providing notices and updates to the Council as required by Va. Code § 2.2-3704.2.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Protected Information

805.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the access, transmission, release, and security of protected information by members of the Madison County Sheriff's Office. The essential premise of the Criminal Justice Information Services (CJIS) Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This policy applies to every individual - contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity - with access to, or who operates in support of, criminal justice services and information. This policy addresses the protected information that is used in the day-to-day operation of the Department and not the public records information covered in the Records Maintenance and Release Policy.

805.1.1 DEFINITIONS

Definitions related to this policy include:

Contracting Government Agency (CGA) - A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

Criminal Justice Information (CJI) - Criminal Justice Information is the term used to refer to all of the FBI CJIS-provided data necessary
for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

Terminal Agency Coordinator (TAC) -The TAC serves as the point of contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

Agency Coordinator (AC) - An AC is a staff member of the Contracting Government Agency (CGA) who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing, and all required reports by NCIC.

Local Agency Security Officer (LASO) - Each LASO shall:

(a) . Identify who is using the CSA-approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.

(b) Identify and document how the equipment is connected to the state system.

(c) Ensure that personnel security screening procedures are being followed as stated in this Policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Ensure the approved and appropriate security measures are in place and working as expected.

(e) Support policy compliance and ensure the CJI Systems Agency Information Security Officer (CSA ISO) is promptly informed of security incidents.

Protected information - Any information or data that is collected, stored, or accessed by members of the Madison County Sheriff's Office and is subject to any access or release restrictions imposed by law, regulation, order, or use agreement. This includes all information contained in federal, state, or local law enforcement databases that is not accessible to the public.

805.2 POLICY

Members of the Madison County Sheriff's Office will adhere to all applicable laws, orders, regulations, use agreements and training related to the access, use, dissemination and release of protected information.

805.3 RESPONSIBILITIES

The Sheriff shall select a member of the Department to act as the Terminal Agency Coordinator (TAC), Agency Coordinator (AC), and Local Agency Security Officer (LASO) to coordinate the use of protected information.

The responsibilities of these positions include but are not limited to:

(a) Ensuring member compliance with this policy and with requirements applicable to protected information, including requirements for the National Crime Information Center (NCIC) system, National Law Enforcement Telecommunications System (NLETS), and Department of Motor Vehicles (DMV) records.

(b) Developing, disseminating, and maintaining procedures that adopt or comply with the U.S. Department of Justice's current Criminal Justice Information Services (CJIS) Security Policy.

(c) Developing, disseminating, and maintaining any other procedures necessary to comply with any other requirements for the access, use, dissemination, release, and security of protected information (Va. Code § 9.1-130; Va. Code § 19.2-389; Va. Code § 19.2-389.1; Va. Code § 38.2-613(B)(5); 6 VAC 20-120-50; 6 VAC 20-120-60).

(d) Developing procedures to ensure training and certification requirements are met.

(e) Resolving specific questions that arise regarding authorized recipients of protected information.

(f) Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.

See attachment: 805 CJIS Security Policy Rev. 5.9.pdf

Virginia State Police Criminal Justice Information Services CJIS Section

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Protected Information

805.4 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, Madison County Sheriff's Office policy or training. Only those members who have completed applicable training and met any applicable requirements, such as a background check, may access protected information, and only when the member has a legitimate work-related reason for such access.

Unauthorized access, including access for other than a legitimate work-related purpose, is prohibited and may subject a member to administrative action pursuant to the Personnel Complaints Policy and/or criminal prosecution.

805.5 RELEASE OR DISSEMINATION OF PROTECTED INFORMATION

Protected information may be released only to authorized recipients who have both a right to know and a need to know.

A member who is asked to release protected information that should not be released should refer the requesting person to a supervisor or to the Records Manager for information regarding a formal request.

Unless otherwise ordered or when an investigation would be jeopardized, protected information maintained by the Department may generally be shared with authorized persons from other law enforcement agencies who are assisting in the investigation or conducting a related investigation. Any such information should be released through the Records Division to ensure proper documentation of the release (see the Records Maintenance and Release Policy).

Protected information, such as Criminal Justice Information (CJI), which includes Criminal History Record Information (CHRI), should generally not be transmitted by radio, cellular telephone or any other type of wireless transmission to members in the field or in vehicles through any computer or electronic device, except in cases where there is an immediate need for the information to further an investigation or where circumstances reasonably indicate that the immediate safety of deputies, other department members or the public is at risk.

Nothing in this policy is intended to prohibit broadcasting warrant information.

805.5.1 REVIEW OF CRIMINAL HISTORY RECORD

A person whose criminal history record is maintained by this department has the right to inspect a copy of his/her information at the Department for the purpose of ascertaining the completeness and accuracy of the information. For offenses that are required to be reported to the Central Criminal Records Exchange (CCRE), the requester shall be referred to the CCRE. For offenses that are non-reportable to CCRE, the Department shall provide the information requested following the dissemination procedures as required by 6 VAC 20-120-50 (Va. Code § 9.1-132).

805.6 SECURITY OF PROTECTED INFORMATION

The Sheriff will select a member of the Department to act as the Local Agency Security Officer (LASO) and to oversee the security of protected information.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

The responsibilities of the LASO include but are not limited to:

(a) Developing and maintaining security practices, procedures, and training.

(b) Ensuring federal and state compliance with the CJIS Security Policy and the requirements of any state or local criminal history records systems.

(c) Establishing procedures to provide for the preparation, prevention, detection, analysis, and containment of security incidents including computer attacks.

(d) Tracking, documenting, and reporting all breach of security incidents to the Sheriff and appropriate authorities (Va. Code § 2.2-5514).

805.6.1 MEMBER RESPONSIBILITIES

Members accessing or receiving protected information shall ensure the information is not accessed or received by persons who are not authorized to access or receive it. This includes leaving protected information, such as documents or computer databases, accessible to others when it is reasonably foreseeable that unauthorized access may occur (e.g., on an unattended table or desk, in or on an unattended vehicle, in an unlocked desk drawer or file cabinet, on an unattended computer terminal).

805.7 TRAINING

All members authorized to access or release protected information shall complete a training program that complies with any applicable local, state and federal CJIS protected information system requirements and identifies authorized access and use of protected information, as well as its proper handling and dissemination.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Animal Control

806.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for interacting with animals and responding to calls for service that involve animals.

806.2 POLICY

It is the policy of the Madison County Sheriff's Office to be responsive to the needs of the community regarding animal-related issues. This includes enforcing local, state and federal laws relating to animals and appropriately resolving or referring animal-related problems, as outlined in this policy.

Deputies shall enforce laws relating to animals to the same extent that other laws in the Commonwealth of Virginia are enforced (Va. Code § 3.2-6567).

806.3 ANIMAL CONTROL RESPONSIBILITIES

Animal control services are generally the primary responsibility of Madison County, Virginia Animal Control (MCAC) and include the following:

(a) Ongoing or persistent animal nuisance complaints.

(b) Follow-up on animal-related calls, such as locating owners of injured animals.

806.4 MEMBER RESPONSIBILITIES

Members who respond to or assist with animal-related calls for service should evaluate the situation to determine appropriate actions to control the situation.

Due to the hazards of handling animals without proper training and equipment, responding members generally should not attempt to capture or pick up any animal, but should keep the animal under observation until the arrival of appropriate assistance.

Members may consider acting before the arrival of such assistance when:

(a) There is a threat to public safety.

(b) An animal has bitten someone. Members should take measures to confine the animal and prevent further injury.

(c) An animal is creating a traffic hazard.

(d) An animal is seriously injured. In this case, deputies will contact the Virginia Department of Transportation (VDOT) for removal of the carcass.

(e) The owner/handler of an animal has been arrested or is incapacitated. In such circumstances, the member should find appropriate placement for the animal.

1. This is only necessary when the arrestee is expected to be in custody for a time period longer than would reasonably allow him/her to properly care for the animal.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. With the owner's consent, locating appropriate placement may require contacting relatives or neighbors to care for the animal.
3. If no person can be found or the owner does not or cannot give consent, the animal should be taken to a designated animal care facility.

(f) A dangerous or vicious dog is found in violation of Va. Code § 3.2-6540 or Va. Code § 3.2-6540.1.

806.4.1 STATE REQUIREMENTS

Members taking custody of a dog or a cat shall ask whether, if known, the animal has bitten a person or other animal, and the date and circumstances of such bite. Members shall document the information in the report of the incident.

Members who subsequently release the animal for adoption, return to rightful owner, or transfer to another agency shall disclose that the animal has bitten a person or other animal and the circumstances and date of such bite (Va. Code § 3.2-6509.1).

806.5 ANIMAL CRUELTY COMPLAINTS

Laws relating to the cruelty to animals should be investigated by Madison County, Virginia Animal Control. This Department should assist as needed. Areas of enforcement including, but are not limited to:

(a) Care of companion animals by owner (Va. Code § 3.2-6503).
(b) Care of agricultural animals by owner (Va. Code § 3.2-6503.1).
(c) Abandonment of animal (Va. Code § 3.2-6504).
(d) Cruelty to animals (Va. Code § 3.2-6570 et seq.).
(e) Control of dangerous dogs (Va. Code § 3.2-6540).
(f) Control of vicious dogs (Va. Code § 3.2-6540.1).

MCAC should conduct an investigation on all reports of animal cruelty. Legal steps should be taken to protect an animal that is in need of immediate care or protection from acts of cruelty (Va. Code § 3.2-6564).

806.6 ANIMAL BITE REPORTS

Members investigating an animal bite should obtain as much information as possible for follow-up with the appropriate health or animal authorities. Efforts should be made to capture or otherwise have the animal placed under control. Members should attempt to identify and notify the owner of the final disposition of the animal.

806.7 STRAY DOGS

If the dog has a license or can otherwise be identified, the owner should be contacted, if possible. If the owner is contacted, the dog should be released to the owner and a citation may be issued, if appropriate. If a dog is taken into custody, it shall be transported to the appropriate shelter/ holding pen.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Members shall provide reasonable treatment to animals in their care (e.g., food, water, shelter).

806.8 DANGEROUS ANIMALS

In the event responding members cannot fulfill a request for service because an animal is difficult or dangerous to handle, the Shift Supervisor will be contacted to determine available resources, including requesting the assistance of animal control services from an allied agency.

806.9 PUBLIC NUISANCE CALLS RELATING TO ANIMALS

Members should diligently address calls related to nuisance animals (e.g., barking dogs), because such calls may involve significant quality-of-life issues.

806.10 DECEASED ANIMALS

When a member becomes aware of a deceased animal, all reasonable attempts should be made to preliminarily determine if the death of the animal is related to criminal activity.

Deceased animals on public property should be removed, sealed in a plastic bag and properly disposed of by the responding member.

Members should not climb onto or under any privately owned structure for the purpose of removing a deceased animal.

806.11 INJURED ANIMALS

When a member becomes aware of an injured domesticated animal, all reasonable attempts should be made to contact an owner or responsible handler. If an owner or responsible handler cannot be located, MCAC should be notified.

806.11.1 VETERINARY CARE

When the owner or responsible handler cannot be located and the animal is not an immediate danger to the community, it shall be taken to a veterinarian as described below:

Members are authorized to impound and take any animal to a veterinarian when the animal (Va. Code § 3.2-6569):

(a) Has been abandoned.

(b) Has been cruelly treated.

(c) Is suffering a direct and immediate threat to its life, safety or health.

Prior to seizing or impounding any agricultural animal, members shall contact the State Veterinarian who shall recommend the most appropriate action for effecting the seizure or impoundment (Va. Code § 3.2-6569).

806.12 DESTRUCTION OF ANIMALS

When it is necessary to use a firearm to euthanize a badly injured animal or stop an animal that poses an imminent threat to human safety, the Firearms Policy shall be followed. A badly injured animal shall only be euthanized with the approval of a supervisor.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

When practicable, the assistance of a humane investigator should be obtained to handle the euthanasia of an animal (Va. Code § 3.2-6558; Va. Code § 3.2-6563).

Animal Control or deputies may kill a dog that is in the act of killing or injuring livestock or poultry (Va. Code § 3.2-6552).

806.13 REPORTS

Members who take an animal into custody should generate a complete report of the incident, including a description of the animal (species, color, breed, sex, approximate age and weight, and temperament), the reason the animal was taken into custody, the animal's home address, if known, and any identification number, tag information or other identification on the animal (Va. Code § 3.2-6557).

The Sheriff or the authorized designee should ensure that this policy and any animal intake procedures are filed annually with the State Veterinarian's Office (Va. Code § 3.2-6557).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Courthouse Security Operations

807.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the physical security of court facilities, and for the personal security of the officers, employees and the public having business to conduct on the premises.

807.2 POLICY

It is the policy of the Madison County Sheriff's Office to provide for the physical security of court facilities under department/office control, and to employ available resources to promote the safety of judicial officers, court staff, attorneys, litigants, witnesses, prisoners, the public, and assigned department/office personnel on the premises.

The Madison County Sheriff's Office respects the rights of people to access public buildings. It is the policy of this department not to unreasonably interfere with, harass, intimidate or discriminate against persons engaged in the lawful exercise of their rights, while preserving the peace, protecting life and preventing the destruction of property.

807.3 RESPONSIBILITIES

Deputies should be mindful of their responsibility to protect themselves and the public from any potential physical threats.

Assigned deputies are responsible for ensuring that all court facilities remain secure from unauthorized access at all times. All exterior doors should remain closed and locked at all times unless there are secondary barriers or a deputy is present to prevent unauthorized access. All persons entering the court facility are subject to search.

The Sheriff shall assign a Division Supervisor the responsibility for administering and managing the court security function of the Madison County Sheriff's Office.

Department members should apply the following guidelines whenever practicable.

807.3.1 PUBLIC ACCESS AREAS

Public access to court facilities should only be permitted during established business hours and only when staffing is available to adequately monitor the movement of persons within the facility and to restrict access to non-public and secure areas. The court facility should have a designated entry area and established procedures for screening users of the facility for weapons and contraband.

807.3.2 FACILITY ACCESS CONTROL

An entry control process, including physical barriers should exist at each court facility, including those with public access. All persons entering the court facility should be screened for weapons at the time of entry. There may be varying degrees of access established with different access and escort requirements. Access categories may include, but are not limited to:

- Judges and Magistrates

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

- Court employees
- Attorneys
- On-duty law enforcement officers
- Emergency service providers
- Contractors and vendors
- Jurors
- Members of the public

Facility security includes. but is not limited to:

- Interior and exterior doors
- Windows and lighting
- Emergency power, fire/smoke detection and suppression equipment
- All types of alarms
- Key control
- Secure areas
- Circulation patterns
- Communications
- Restricted areas
- Access for persons with disabilities

807.3.3 EQUIPMENT

All equipment that is property of the Madison County Sheriff's Office shall be maintained according to the Department-Owned and Personal Property Policy. For the purposes of this policy, department-owned court security equipment includes, but is not limited to:

- Magnetometers
- Parcel X-ray machines
- Handheld metal detecting wands
- Video cameras and monitors
- Alarms
- Medical supplies
- Fire suppression equipment
- Restraining devices
- Communications equipment

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

807.3.4 FACILITY SURVEY

The Madison County Sheriff's Office shall develop and implement a court facility emergency management plan. The court facility emergency management plan should be established pursuant to the results of a site survey of the court facility. The site survey should be conducted every three years.

The court facility emergency management plan should include, but is not limited to:

- Emergencies (e.g., fire, medical, hostage, bomb, disaster)
- High-risk trials and other court proceedings
- Weapons
- Use of restraining devices
- Detainee movement and circulation patterns
- Lockdown
- Evacuation

807.3.5 WEAPONS

The Madison County Sheriff's Office should ensure that weapons and dangerous instruments are excluded from the court facility, unless carried or maintained by those individuals who are authorized by law or as required for facility security. Notice that weapons shall not be possessed or brought into the court facility shall be posted conspicuously at each public entrance to each courthouse or other building containing a court facility.

Lockboxes should be available for the safe, secure and convenient storage of weapons of officers/deputies at the court facility. Officers/deputies storing weapons at a facility shall be provided a receipt for the firearm. Procedures for the safe receipt, handling, storage and return of weapons should be implemented.

807.3.6 COURTROOMS

Courtrooms under the control of the Madison County Sheriff's Office should be equipped with duress alarms that terminate in an area where rapid response can be made by members of the Madison County Sheriff's Office.

807.4 SCREENING PROCESS

(a) All persons entering the secure area of the courts shall be required to pass through a walk-through metal detector or be scanned by a handheld metal detector, or be hand searched prior to entering the secure area. Citizens have the right to refuse the search/scanning process but will be denied entry into the courthouse facility.

(b) Searches are required to prevent contraband or weapons from entering the facilities. This includes anything that which could reasonably be used as a weapon, unauthorized recording devices, or anything that which may be disruptive to court proceedings.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) Special accommodations may be necessary for those who are handicapped, especially if they are confined to a wheelchair or have a prosthetic device. In this or similar situations, a search will be conducted by hand or by using a handheld metal detector, sd appropriate.

(d) All metal items, electronic devices, bags, backpacks, and packages will be scanned by the x-ray machine and searched for contraband or weapons.

(e) Persons other than on-duty, uniformed officers/deputies in possession of weapons or contraband shall be denied entry to the court facility. Screening personnel shall not hold weapons or contraband for safekeeping. Screening personnel will advise persons to remove prohibited items from the court facility or to dispose of such items in the contraband box.

(f) If screening personnel determine that a citizen is attempting to conceal or introduce a deadly/ dangerous weapon into a court facility, the weapon may be seized, and the citizen detained. Appropriate enforcement action will be taken, and the weapon surrendered as evidence.

(g) Judges, law enforcement officers in uniform or otherwise properly identified,or persons with proper access to the court facilities may be excused from the search process.

(h) Law enforcement personnel while attending court for personal business will not be allowed to carry a weapon inside the courthouse.

807.5 BAILIFF RESPONSIBILITIES

Deputies assigned to courtroom as security duties during judicial proceedings will be designated as bailiffs and act at the direction of the presiding judge. Bailiffs will be responsible for:

(a) Ensuring the physical security of the judge, courtroom staff, parties and the public

(b) Escorting, and security of prisoners

(c) Maintaining order and decorum in the courtroom and adjacent spaces

(d) Ensuring that the physical security plan is followed

(e) Ensuring that there is no eating, drinking, or smoking in the courtroom

(f) Maintaining control of contraband taken into the courtroom for evidentiary purposes

(g) In the event of an unusual occurrence, assuming control and requesting additional police, fire, or medical assistance, as the circumstances may require

807.5.1 PHYSICAL SECURITY IN THE COURTROOM

The bailiff will make a physical inspection of the courtroom, both prior to and after court proceedings, to ensure that:

(a) The courtroom is free of weapons and contraband

(b) All doors are open and free of obstruction

(c) The duress alarm is in working order

(d) Restraining devices are present

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(e) The door at the rear of the courtroom is unlocked and free of obstructions

807.6 ENFORCEMENT ACTION

Deputiesmay take enforcement action inside a facility, on the grounds surrounding any court facility, and in parking lots adjacent to the court facility. Enforcement actions outside of a court facility should be limited to pursuit or apprehension of persons suspected of criminal activity.

807.7 TRAINING

The Training Supervisor should develop a basic training plan for all members assigned to the court facility. All assigned deputies should complete the basic training program before assuming their court security duties.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Chapter 9 - Custody

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Temporary Custody of Adults

900.1 PURPOSE AND SCOPE

This policy provides guidelines to address the health and safety of adults taken into temporary custody by members of the Madison County Sheriff's Office for processing prior to being released or transferred to a housing or other type of facility.

Temporary custody of juveniles is addressed in the Temporary Custody of Juveniles Policy. Juveniles will not be permitted where adults in custody are being held.

Custodial searches are addressed in the Custodial Searches Policy.

900.1.1 DEFINITIONS

Definitions related to this policy include:

Holding cell/cell - Any locked enclosure for the custody of an adult or any other enclosure that prevents the occupants from being directly visually monitored at all times by a member of the Department.

Safety checks - Direct, visual observation by a member of this department performed at random intervals, within time frames prescribed in this policy, to provide for the health and welfare of adults in temporary custody.

Temporary custody - The period an adult is in custody at the Madison County Sheriff's Office prior to being released or transported to a housing or other type of facility.

900.2 POLICY

The Madison County Sheriff's Office is committed to releasing adults from temporary custody as soon as reasonably practicable, and to keeping adults safe while in temporary custody at the Department. Adults should be in temporary custody only for as long as reasonably necessary for investigation, processing, transfer or release.

900.3 GENERAL CRITERIA AND SUPERVISION

No adult should be in temporary custody for longer than six hours but in no case longer than 12 hours (6 VAC 15-40-10).

900.3.1 INDIVIDUALS WHO SHOULD NOT BE IN TEMPORARY CUSTODY

Individuals who exhibit certain behaviors or conditions should not be in temporary custody at the Madison County Sheriff's Office, but should be transported to a jail facility, a medical facility or other type of facility as appropriate. These include:

(a) Any individual who is unconscious or has been unconscious while being taken into custody or while being transported.

(b) Any individual who has a medical condition, including pregnancy, that may require medical attention, supervision or medication while in temporary custody.

(c) Any individual who is seriously injured.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Individuals who are a suspected suicide risk (see the Civil Commitments Policy).

1. If the deputy taking custody of an individual believes that he/she may be a suicide risk, the deputy shall ensure continuous direct supervision until evaluation, release or a transfer to an appropriate facility is completed.

(e) Individuals who are obviously in crisis, as defined in the Crisis Intervention Incidents Policy.

(f) Individuals who are under the influence of alcohol, a controlled substance or any substance to the degree that may require medical attention, or who have ingested any substance that poses a significant risk to their health, whether or not they appear intoxicated.

(g) Any individual who has exhibited extremely violent or continuously violent behavior.

(h) Any individual who has claimed, is known to be afflicted with or displays symptoms of any communicable disease that poses an unreasonable exposure risk.

(i) Any individual with a prosthetic or orthopedic device where removal of the device would be injurious to his/her health or safety.

Deputies taking custody of a person who exhibits any of the above conditions should notify a supervisor of the situation. These individuals should not be in temporary custody at the Department unless they have been evaluated by a qualified medical or mental health professional, as appropriate for the circumstances.

900.3.2 SUPERVISION IN TEMPORARY CUSTODY

An authorized department member capable of supervising shall be present at all times when an individual is held in temporary custody (6 VAC 15-40-1220). The member responsible for supervising should not have other duties that could unreasonably conflict with his/her supervision. Any individual in custody must be able to summon the supervising member if needed. If the person in custody is deaf or hard of hearing or cannot speak, accommodations shall be made to provide this ability.

At least one female department member should be present when a female adult is in temporary custody. In the event that none is readily available, the shift supervisor should consider whether the female in custody should can be transported to another facility or released pursuant to another lawful process. If none of these options are feasible, the female in custody should be monitored by video at all times. Two sworn deputies should be present if it is necessary to enter the lockup for any reason.

Absent exigent circumstances, such as a medical emergency or a violent subject,members should not enter the cell of a person of the opposite sex unless amember of the same sex as the person in custody is present.

No individual in custody shall be permitted to supervise, control or exert any authority over other individuals in custody.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

900.3.3 ENTRY RESTRICTIONS
Entry into any location where a person is held in custody should be restricted to:

(a) Authorized members entering for official business purposes.

(b) Emergency medical personnel when necessary.

(c) Any other person authorized by the Shift Supervisor.

When practicable, more than one authorized member should be present for entry into a location where a person is held in custody for security purposes and to witness interactions.

900.4 INITIATING TEMPORARY CUSTODY

The deputy responsible for an individual in temporary custody should evaluate the person for any apparent chronic illness, disability, vermin infestation, possible communicable disease or any other potential risk to the health or safety of the individual or others. The deputy should specifically ask if the individual is contemplating suicide and evaluate him/her for obvious signs or indications of suicidal intent.

The receiving deputy should ask the arresting deputy if there is any statement, indication or evidence surrounding the individual's arrest and transportation that would indicate the individual is at risk for suicide or critical medical care. If there is any suspicion that the individual may be suicidal, he/she shall be transported to the Regional jail or the appropriate mental health facility.

The deputy should promptly notify the Shift Supervisor of any conditions that may warrant immediate medical attention or other appropriate action. The Shift Supervisor shall determine whether the individual will be placed in a cell, immediately released or transported to jail or another facility.

900.4.1 SCREENING AND PLACEMENT
The deputy responsible for an individual in custody shall:

(a) Advise the Shift Supervisor of any significant risks presented by the individual (e.g., suicide risk, health risk, violence).

(b) Evaluate the following issues against the stated risks in (a) to determine the need for placing the individual in a single cell:

1. Consider whether the individual may be at a high risk of being sexually abused based on all available known information (28 CFR 115.141), or whether the person is facing any other identified risk.

2. Provide an individual identified as being at a high risk for sexual or other victimization with heightened protection (6 VAC 15-40-1300). This may include (28 CFR 115.113; 28 CFR 115.141):

(a) Continuous, direct sight and sound supervision.

(b) Single-cell placement in a cell that is actively monitored on video by a member who is available to immediately intervene.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

3. Ensure individuals are separated according to severity of the crime (e.g., felony or misdemeanor).
4. Ensure males and females are separated by sight and sound when in cells (6 VAC 15-40-1290).
5. Ensure restrained individuals are not placed in cells with unrestrained individuals.

(c) Ensure that those confined under civil process or for civil causes are kept separate from those who are in temporary custody pending criminal charges.

(d) Ensure separation, as appropriate, based on other factors, such as age, criminal sophistication, assaultive/non-assaultive behavior, mental state, disabilities and sexual orientation.

1. Mentally ill individuals shall not be confined in a cell or room with any prisoners charged or convicted of a crime (VA Code §37.2-832).

900.4.2 CONSULAR NOTIFICATION

Consular notification may be mandatory when certain foreign nationals are arrested. The Patrol Division Supervisor will ensure that the U.S. Department of State's list of countries and jurisdictions that require mandatory notification is readily available to department members. There should also be a published list of foreign embassy and consulate telephone and fax numbers, as well as standardized notification forms that can be transmitted and then retained for documentation. Prominently displayed signs informing foreign nationals of their rights related to consular notification should also be posted in areas used for the temporary custody of adults.

Department members assigned to process a foreign national shall:

(a) Inform the individual, without delay, that he/she may have his/her consular officers notified of the arrest or detention and may communicate with them.

1. This notification should be documented.

(b) Determine whether the foreign national's country is on the U.S. Department of State's mandatory notification list.

1. If the country is on the mandatory notification list, then:
   (a) Notify the country's nearest embassy or consulate of the arrest or detention by fax or telephone.
   (b) Tell the individual that this notification has been made and inform him/her without delay that he/she may communicate with consular officers.
   (c) Forward any communication from the individual to his/her consular officers without delay.
   (d) Document all notifications to the embassy or consulate and retain the faxed notification and any fax confirmation for the individual's file.
2. If the country is not on the mandatory notification list and the individual requests that his/her consular officers be notified, then:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) Notify the country's nearest embassy or consulate of the arrest or detention by fax or telephone.

(b) Forward any communication from the individual to his/her consular officers without delay.

Department of State Consular Notification Guide to Law Enforcement

900.5 SAFETY, HEALTH AND OTHER PROVISIONS

900.5.1 TEMPORARY CUSTODY LOGS

Any time an individual is in temporary custody at the Madison County Sheriff's Office, the custody shall be promptly and properly documented in a custody log, including (6 VAC 15-40-1250):

(a) Identifying information about the individual, including his/her name.

(b) Date and time of arrival at the Department.

(c) Any charges for which the individual is in temporary custody and any case number.

(d) Time of all safety checks.

(e) Any medical and other screening requested and completed.

(f) Any emergency situations or unusual incidents.

(g) Any other information that may be required by other authorities, such as compliance inspectors.

(h) Date and time of release from the Madison County Sheriff's Office.

The Shift Supervisor should initial the log to approve the temporary custody and should also initial the log when the individual is released from custody or transferred to another facility.

The Shift Supervisor should make periodic checks to ensure all log entries and safety and security checks are made on time.

See attachment: Detainee Personal Property Record Receipt.pdf

900.5.2 TEMPORARY CUSTODY REQUIREMENTS

Members monitoring or processing anyone in temporary custody shall ensure:

(a) Safety checks and significant incidents/activities are noted on the log.

(b) Individuals in custody are informed that they will be monitored at all times, except when using the toilet.

1. There shall be no viewing devices, such as peep holes or mirrors, of which the individual is not aware.

2. This does not apply to surreptitious and legally obtained recorded interrogations.

(c) There is reasonable access to toilets and wash basins (6 VAC 15-40-1360).

(d) There is reasonable access to a drinking fountain or water.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(e) There are reasonable opportunities to stand and stretch, particularly if handcuffed or otherwise restrained.

(f) There is privacy during attorney visits (6 VAC 15-40-1330).

(g) Those in temporary custody are generally permitted to remain in their personal clothing unless it is taken as evidence or is otherwise unsuitable or inadequate for continued wear while in custody.

(h) Clean blankets are provided as reasonably necessary to ensure the comfort of an individual.

(i) Adequate shelter, heat, light and ventilation are provided without compromising security or enabling escape.

(j) Adequate furnishings are available, including suitable chairs or benches.

900.5.3 MEDICAL CARE

First-aid equipment and basic medical supplies should be available to department members. At least one member who has current certification in basic first aid and CPR should be on-duty at all times.

Should a person in custody be injured or become ill, appropriate medical assistance should be sought. A supervisor shall meet with those providing medical aid at the facility to allow access to the person. Members shall comply with the opinion of medical personnel as to whether an individual in temporary custody should be transported to the hospital. If the person is transported while still in custody, he/she will be accompanied by a deputy.

Those who require medication while in temporary custody should not be at the Madison County Sheriff's Office. They should be released or transferred to another facility as appropriate.

900.5.4 ORTHOPEDIC OR PROSTHETIC APPLIANCE

Subject to safety and security concerns, individuals shall be permitted to retain an orthopedic or prosthetic appliance. However, if the appliance presents a risk of bodily harm to any person or is a risk to the security of the facility, the appliance may be removed from the individual unless its removal would be injurious to his/her health or safety.

Whenever a prosthetic or orthopedic appliance is removed, the Shift Supervisor shall be promptly apprised of the reason. It shall be promptly returned when it reasonably appears that any risk no longer exists.

900.5.5 TELEPHONE CALLS

Every individual in temporary custody shall be allowed to make a reasonable number of completed telephone calls (but at least two) as soon as possible after arrival (6 VAC 15-40-1270).

(a) Telephone calls may be limited to local calls, except that long-distance calls may be made by the individual at his/her own expense.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1. The Department should pay the cost of any long-distance calls related to arranging for the care of a child or dependent adult (see the Child and Dependent Adult Safety Policy).

(b) The individual should be given sufficient time to contact whomever he/she desires and to make any necessary arrangements, including child or dependent adult care, or transportation upon release.

1. Telephone calls are not intended to be lengthy conversations. The member assigned to monitor or process the individual may use his/her judgment in determining the duration of the calls.

(c) Calls between an individual in temporary custody and his/her attorney shall be deemed confidential and shall not be monitored, eavesdropped upon or recorded.

(d) Reasonable accommodations shall be made for non-English speaking detainees as well as hearing and visually impaired detainees.

900.5.6 RELIGIOUS ACCOMMODATION

Subject to available resources, safety and security, the religious beliefs and needs of all individuals in custody should be reasonably accommodated. Requests for religious accommodation should generally be granted unless there is a compelling security or safety reason and denying the request is the least restrictive means available to ensure security or safety. The responsible supervisor should be advised any time a request for religious accommodation is denied.

Those who request to wear headscarves or simple head coverings for religious reasons should generally be accommodated absent unusual circumstances. Head coverings shall be searched before being worn.

Individuals wearing headscarves or other approved coverings shall not be required to remove them while in the presence of or while visible to the opposite sex if they so desire. Religious garments that substantially cover the individual's head and face may be temporarily removed during the taking of any photographs.

900.5.7 FIREARMS AND OTHER SECURITY MEASURES

Firearms and other weapons and control devices shall not be permitted in secure areas where individuals are in custody or are processed. They should be properly secured outside of the secure area. An exception may occur only during emergencies, upon approval of a supervisor.

All perimeter doors to secure areas shall be kept locked at all times, except during routine cleaning, when no individuals in custody are present or in the event of an emergency, such as an evacuation.

900.5.8 DISCIPLINE

Punishment shall not be used to control an adult in custody (6 VAC 15-40-1340).

900.5.9 ESCAPES

Upon being made aware that an escape may have occurred, or did in fact occur, the member should immediately notify the Dispatch Center. the Dispatch Center should notify the Shift

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Supervisor and other members about the escape. As soon as practicable, the Shift Supervisor should notify the Sheriff.

Once the escape is verified and immediate actions taken inside the facility, the Shift Supervisor should notify other appropriate law enforcement agencies. Appropriate investigative and search measures should be taken to apprehend the escapee.

The Shift Supervisor or a designated member should submit a report through the chain of command to the Sheriff as soon as practicable.

900.6 USE OF RESTRAINT DEVICES

Individuals in custody may be handcuffed in accordance with the Handcuffing and Restraints Policy. Unless an individual presents a heightened risk, handcuffs should generally be removed when the person is in a cell.

The use of restraints, other than handcuffs or leg irons, generally should not be used for individuals in temporary custody at the Madison County Sheriff's Office unless the person presents a heightened risk, and only in compliance with the Handcuffing and Restraints Policy.

Individuals in restraints shall be kept away from other unrestrained individuals in custody and monitored to protect them from abuse.

900.6.1 PREGNANT ADULTS

Women who are known to be pregnant should be restrained in accordance with the Handcuffing and Restraints Policy.

900.7 PERSONAL PROPERTY

The personal property of an individual in temporary custody should be removed, inventoried and processed as provided in the Custodial Searches Policy, unless the individual requests a different disposition. For example, an individual may request property (e.g., cash, car or house keys, medications) be released to another person. A request for the release of property to another person must be made in writing. Release of the property requires the recipient's signature on the appropriate form.

Upon release of an individual from temporary custody, his/her items of personal property shall be compared with the inventory, and he/she shall sign a receipt for the property's return. If the individual is transferred to another facility or court, the member transporting the individual is required to obtain the receiving person's signature as notice of receipt. The Department shall maintain a copy of the property receipt.

The Shift Supervisor shall be notified whenever an individual alleges that there is a shortage or discrepancy regarding his/her property. The Shift Supervisor shall attempt to prove or disprove the claim.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

900.8 HOLDING CELLS

A thorough inspection of a cell shall be conducted before placing an individual into the cell to ensure there are no weapons or contraband and that the cell is clean and sanitary. An inspection also should be conducted when he/she is released. Any damage noted to the cell should be photographed and documented.

The following requirements shall apply:

(a) The individual shall be searched (see the Custodial Searches Policy) and anything that could create a security or suicide risk, such as contraband, hazardous items, belts, shoes or shoelaces, and jackets, shall be removed.

(b) The individual shall constantly be monitored by an audio/video system during the entire custody.

(c) The individual shall have constant auditory access to department members.

(d) The individual's initial placement into and removal from a locked enclosure shall be logged.

(e) Safety checks by department members shall occur no less than every 15 minutes (6 VAC 15-40-1315).

1. Safety checks should be at varying times.
2. All safety checks shall be logged.
3. The safety check should involve questioning the individual as to his/her well-being.
4. Individuals who are sleeping or apparently sleeping should be awakened.
5. Requests or concerns of the individual should be logged.
6. Obstructions preventing staff from being able to see the entire cell shall be removed.

900.9 SUICIDE ATTEMPT, DEATH OR SERIOUS INJURY

The Patrol Division Supervisor will ensure procedures are in place to address any suicide attempt, death or serious injury of any individual in temporary custody at the Madison County Sheriff's Office. The procedures should include:

(a) Immediate request for emergency medical assistance if appropriate.

(b) Immediate notification of the Shift Supervisor, Sheriff and Investigation Division Supervisor.

(c) Notification of the spouse, next of kin or other appropriate person.

(d) Notification of the appropriate prosecutor.

(e) Notification of the County Attorney.

(f) Notification of the Medical Examiner.

(g) Evidence preservation.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(h) Initial report of death to the local facilities supervisor or designee of the Compliance and Accreditation Unit, Department of Corrections within 24 hours (6 VAC 15-40-1350).

900.10 RELEASE AND/OR TRANSFER

When an individual is released or transferred from custody, the member releasing the individual should ensure:

(a) All proper reports, forms and logs have been completed prior to release.

(b) A check has been made to ensure that the individual is not reported as missing and does not have outstanding warrants.

(c) It has been confirmed that the correct individual is being released or transported.

(d) All property, except evidence, contraband or dangerous weapons, has been returned to, or sent with, the individual.

(e) All pertinent documentation accompanies the individual being transported to another facility (e.g., copies of booking forms, medical records, an itemized list of his/her property, warrant copies).

(f) The individual is not permitted in any nonpublic areas of the Madison County Sheriff's Office unless escorted by a member of the Department.

(g) Any known threat or danger the individual may pose (e.g., escape risk, suicide potential, medical condition) is documented, and the documentation transported with the individual if he/she is being sent to another facility.

1. The department member transporting the individual shall ensure such risks are communicated to intake personnel at the other facility.

(h) Generally, persons of the opposite sex, or adults and juveniles, should not be transported in the same vehicle unless they are physically separated by a solid barrier. If segregating individuals is not practicable, deputies should be alert to inappropriate physical or verbal contact and take appropriate action as necessary.

(i) Transfers between facilities or other entities, such as a hospital, should be accomplished with a custodial escort of the same sex as the person being transferred to assist with his/her personal needs as reasonable.

900.10.1 ESCAPE DURING TRANSPORT

The Patrol Division Supervisor will ensure procedures are in place to address any escape of an individual during transport by the Madison County Sheriff's Office. The procedures should include:

(a) Further actions to be taken by the deputies conducting the transport.

(b) Notifications of the escape.

(c) Written reports by the deputies conducting the transport.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

900.11 ASSIGNED ADMINISTRATOR

The Patrol Division Supervisor will ensure any reasonably necessary supplemental procedures are in place to address the following issues:

(a) General security

(b) Key control

(c) Sanitation and maintenance (6 VAC 15-40-1370)

(d) Emergency medical treatment (6 VAC 15-40-1310)

(e) Escapes

(f) Evacuation plans

(g) Fire and life-safety

(h) Disaster plans

(i) Building and safety code compliance

(j) Documentation of serious events related to adults in custody (6 VAC 15-40-1350)

(k) Mental health care (6 VAC 15-40-1310)

(l) Photographing and fingerprinting, and reports to the Virginia Central Criminal Records Exchange, as required by state law (Va. Code § 19.2-390)

900.12 TRAINING

Department members should be trained and familiar with this policy and any supplemental procedures.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Temporary Custody of Juveniles

901.1 PURPOSE AND SCOPE

This policy provides guidelines consistent with the Juvenile Justice and Delinquency Prevention Act for juveniles taken into temporary custody by members of the Madison County Sheriff's Office (34 USC § 11133).

901.1.1 DEFINITIONS

Definitions related to this policy include:

Juvenile non-offender - An abused, neglected, dependent, or alien juvenile who may be legally held for the juvenile's own safety or welfare. This also includes any juvenile who may have initially been contacted for an offense that would not subject an adult to arrest (e.g., fine-only offense) but was taken into custody for the juvenile's protection or for purposes of reuniting the juvenile with a parent, guardian, or other responsible person.

Juvenile offender - A juvenile 17 years of age or younger who is alleged to have committed an offense that would subject an adult to arrest (a non-status offense). It also includes unlawful possession or transportation of a handgun or assault firearms under Va. Code § 18.2-308.7 (28 CFR 31.303).

Non-secure custody - When a juvenile is held in the presence of a deputy or other department member at all times and is not placed in a locked room, cell, or behind any locked doors. Juveniles in non-secure custody may be handcuffed but not to a stationary or secure object. Personal supervision, through direct visual monitoring and audio two-way communication, is maintained. Monitoring through electronic devices, such as video, does not replace direct visual observation.

Safety checks - Direct visual observation by a member of this department performed at random intervals, within time frames prescribed in this policy, to provide for the health and welfare of juveniles in temporary custody.

Secure custody - When a juvenile offender is held in a locked room, a set of rooms, or a cell. Secure custody also includes being physically secured to a stationary object.

Examples of secure custody include:

(a) A juvenile left alone in an unlocked room within the secure perimeter of the adult temporary holding area.

(b) A juvenile handcuffed to a rail.

(c) A juvenile placed in a room that contains doors with delayed egress devices that have a delay of more than 30 seconds.

(d) A juvenile being processed in a secure booking area when a non-secure booking area is available.

(e) A juvenile left alone in a secure booking area after being photographed and fingerprinted.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(f) A juvenile placed in a cell within the adult temporary holding area, whether or not the cell door is locked.

(g) A juvenile placed in a room that is capable of being locked or contains a fixed object designed for cuffing or restricting movement.

Sight and sound separation - Located or arranged to prevent physical, visual, or auditory contact.

Status offender - A juvenile suspected of committing a criminal violation of the law that would not be a criminal violation but for the age of the offender. Examples may include running away, underage possession of tobacco, curfew violation, and truancy. A juvenile in custody on a court order or warrant based upon a status offense is also a status offender. The term status offender includes a child in need of supervision and a child in need of services as defined in Va. Code § 16.1-228.

901.2 POLICY

The Madison County Sheriff's Office is committed to releasing juveniles from temporary custody as soon as reasonably practicable and to keeping juveniles safe while in temporary custody at the Department. Juveniles should be held in temporary custody only for as long as reasonably necessary for processing, transfer, or release.

The Madison County Sheriff's Office is committed to the development and perpetuation of programs designated to prevent and control juvenile delinquency.

901.3 JUVENILES WHO SHOULD NOT BE HELD

Juveniles who exhibit certain behaviors or conditions should not be held at the Madison County Sheriff's Office. These include:

(a) Unconsciousness or having been unconscious while being taken into custody or transported.

(b) Serious injuries or a medical condition requiring immediate medical attention.

(c) A suspected suicide risk or showing obvious signs of severe emotional or mental disturbance (see the Civil Commitments Policy).

1. If the deputy taking custody of a juvenile believes that he/she may be a suicide risk, the deputy shall ensure continuous direct supervision until evaluation, release, or transfer to an appropriate facility is completed.

(d) Significant intoxication or showing signs of having ingested any substance that poses a significant risk to their health, whether or not they appear intoxicated.

(e) Extremely violent or continuously violent behavior.

(f) Afflicted with, or displaying symptoms of, a communicable disease that poses an unreasonable exposure risk.

Deputies taking custody of a juvenile exhibiting any of the above conditions should take reasonable steps to provide medical attention or mental health assistance and should notify a supervisor of the

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

situation. These juveniles should not be held at the Department unless they have been evaluated by a qualified medical or mental health professional, as appropriate for the circumstances.

901.4 CUSTODY OF JUVENILES

Deputies should take custody of a juvenile and temporarily hold the juvenile at the Madison County Sheriff's Office when there is no other lawful and practicable alternative to temporary custody. Refer to the Child Abuse Policy for additional information regarding detaining a juvenile who is suspected of being a victim.

No juvenile should be held in temporary custody at the Department without authorization of the arresting deputy's supervisor or the Shift Supervisor. Juveniles taken into custody shall be held in non-secure custody unless otherwise authorized by this policy.

Any juvenile taken into custody shall be released to the care of the juvenile’s parent, legal guardian, or other responsible adult, or transferred to a juvenile custody facility or to other authority as soon as practicable. In no event shall a juvenile be held beyond six hours from the time of his/her entry into the Department (34 USC § 11133).

901.4.1 CUSTODY OF JUVENILE NON-OFFENDERS

Non-offenders taken into protective custody in compliance with the Child Abuse Policy should generally not be held at the Madison County Sheriff's Office. Custodial arrangements should be made for non-offenders as soon as reasonably possible. Juvenile non-offenders may not be held in secure custody (34 USC § 11133).

901.4.2 CUSTODY OF JUVENILE STATUS OFFENDERS

Status offenders should generally be released on a summons or with a warning rather than taken into temporary custody. However, deputies may take custody of a status offender if requested to do so by a parent or legal guardian in order to facilitate reunification (e.g., transported home or to the station to await a parent). Juvenile status offenders may not be held in secure custody (34 USC § 11133).

A juvenile who has run away should be released to the institution, facility, or residence from which he/she ran away. If not released, the deputy should contact an intake officer to determine whether the juvenile should be detained pursuant to a warrant or detention order (Va. Code § 16.1-247).

901.4.3 CUSTODY OF JUVENILE OFFENDERS

Juvenile offenders should be held in non-secure custody while at the Madison County Sheriff's Office unless another form of custody is authorized by this policy or is necessary due to exigent circumstances.

(a) Juvenile offenders may be taken into custody under the following circumstances (Va. Code § 16.1-246):

1. When the juvenile has committed a crime in the presence of a deputy and the deputy believes that custody is necessary for the protection of the public interest.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. When the deputy has probable cause based on the reasonable complaint of a person who observed the misdemeanor offense of:
    (a) Shoplifting in violation of Va. Code § 18.2-103.
    (b) Assault and battery.
    (c) Carrying a weapon on school property in violation of Va. Code § 18.2-308.1.
3. When the deputy has probable cause to believe that the juvenile has committed an offense which if committed by an adult would be a felony.
4. Pursuant to a detention order or warrant.

(b) Juvenile offenders should be released to a responsible adult unless there is reason to believe the juvenile offender (Va. Code § 16.1-248.1):

1. Committed an act that would be a felony or Class 1 misdemeanor committed by an adult and either:
    (a) There appears to be a threat to the juvenile, property, or others.
    (b) The juvenile has threatened to abscond or has a record of failing to appear at court hearings within the prior year.
2. Violated the terms of their probation or parole that was based on a felony or Class 1 misdemeanor charge and either:
    (a) There appears to be a threat to the juvenile, property, or others.
    (b) The juvenile has threatened to abscond or has a record of failing to appear at court hearings within the prior year.
3. Possessed or transported a firearm in violation of Va. Code § 18.2-308.7 and either:
    (a) There appears to be a threat to the juvenile, property, or others.
    (b) The juvenile has threatened to abscond or has a record of failing to appear at court hearings within the prior year.
4. Has absconded from a detention facility.
5. Is a fugitive from another state.
6. Has failed to appear in court.
7. Is also in need of supervision.

If the juvenile offender is not released, the deputy shall contact the intake officer and provide the intake officer written notice, including the reasons the juvenile was taken into custody, and shall also ensure notice is given to the juvenile’s parent, guardian, legal custodian, or other person standing in loco parentis.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

901.4.4 ALTERNATIVES TO TEMPORARY CUSTODY
Deputies handling juvenile offenders should use the least coercive, reasonable alternatives to custody, including:

(a) Release to a parent, legal guardian, or other responsible adult, with no further action.

(b) Issuance of a summons or complaint as a referral to the juvenile court.

(c) Referral to juvenile court.

901.4.5 CONSIDERATIONS
When considering appropriate alternatives to temporary custody, several factors should be taken into consideration. These factors include but are not limited to the following:

(a) The nature of the offense

(b) The juvenile's age

(c) The juvenile's prior contacts with law enforcement

(d) The availability of an appropriate juvenile diversion program

(e) The recommendation of the complainant or victim

901.5 ADVISEMENTS
Juveniles are entitled to *Miranda* warnings the same as adults. Deputies should consider whether the age, mental capacity, education, or experience warrant explaining these rights in the presence of a parent or other responsible adult.

901.6 NOTICE TO SCHOOLS
The Sheriff or the authorized designee should disclose to the school principal that a juvenile is a suspect or has been charged with any of the following (Va. Code § 16.1-301):

(a) A violent juvenile felony specified in subsections B and C of Va. Code § 16.1-269.1

(b) A violation of any of the provisions of Va. Code § 18.2-77 et seq. (arson-related crimes)

(c) A violation of law involving any weapon as described in subsection Va. Code § 18.2-308(A)

(d) Any of the crimes described in subsection G of Va. Code § 16.1-260

The member making the disclosure is responsible for ensuring notice is provided to the principal within the time frames provided in Va. Code § 16.1-301.

Additionally, a deputy shall report to the principal of a school, or the principal's designee, the commission of any of the offenses covered under Va. Code § 22.1-279.3:1 when any such offense is committed by a student enrolled at the school.

901.7 JUVENILE CUSTODY LOGS
Any time a juvenile is in temporary custody at the Madison County Sheriff's Office, the custody shall be promptly and properly documented in the juvenile custody log, including:

(a) Identifying information about the juvenile.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Date and time of arrival and release from the Department.

(c) Shift Supervisor notification and approval to temporarily hold the juvenile.

(d) Any charges for which the juvenile is being held and classification of the juvenile as a juvenile offender, status offender, or non-offender.

(e) Any changes in status (e.g., emergency situations, unusual incidents).

(f) Time of all safety checks.

(g) Any medical and other screening requested and completed.

(h) Circumstances that justify any secure custody.

(i) Any other information that may be required by other authorities, such as compliance inspectors or a local juvenile court authority.

The Shift Supervisor should initial the log to approve the temporary custody, including any secure custody, and should initial the log when the juvenile is released.

901.8 NO-CONTACT REQUIREMENTS

Sight and sound separation shall be maintained between all juveniles and adults while in custody at the Madison County Sheriff's Office (34 USC § 11133). There should also be sight and sound separation between non-offenders and juvenile and status offenders.

In situations where brief or accidental contact may occur (e.g., during the brief time a juvenile is being fingerprinted and/or photographed in booking), a member of the Department shall maintain a constant, immediate, side-by-side presence with the juvenile or the adult to minimize any contact. If inadvertent or accidental contact does occur, reasonable efforts shall be taken to end the contact.

901.9 TEMPORARY CUSTODY REQUIREMENTS

Members and supervisors assigned to monitor or process any juvenile at the Madison County Sheriff's Office shall ensure:

(a) The Shift Supervisor is notified if it is anticipated that a juvenile may need to remain at the Department more than four hours. This will enable the Shift Supervisor to ensure no juvenile is held at the Department more than six hours.

(b) Safety checks and significant incidents/activities are noted on the log.

(c) Juveniles in custody are informed that they will be monitored at all times, except when using the toilet.

1. There shall be no viewing devices, such as peep holes or mirrors, of which the juvenile is not aware.

2. This does not apply to surreptitious and legally obtained recorded interrogations.

(d) A member of the same sex will supervise personal hygiene activities and care, such as changing clothing or using the restroom, without direct observation to allow for privacy.

(e) There is reasonable access to toilets and wash basins.

(f) There is reasonable access to a drinking fountain or water.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(g) Food is provided if a juvenile has not eaten within the past four hours or is otherwise in need of nourishment, including any special diet required for the health of the juvenile.

(h) There are reasonable opportunities to stand and stretch, particularly if handcuffed or otherwise restrained.

(i) There is privacy during family, guardian, and/or attorney visits.

(j) Juveniles are generally permitted to remain in their personal clothing unless it is taken as evidence or is otherwise unsuitable or inadequate for continued wear while in custody.

(k) Clean blankets are provided as reasonably necessary to ensure the comfort of an individual.

(l) Adequate shelter, heat, light, and ventilation are provided without compromising security or enabling escape.

(m) Adequate furnishings are available, including suitable chairs or benches.

(n) Juveniles have the right to the same number of telephone calls as adults in temporary custody (see the Temporary Custody of Adults Policy).

(o) Discipline is not administered to any juvenile, nor will juveniles be subjected to corporal or unusual punishment, humiliation, or mental abuse.

901.10 RELIGIOUS ACCOMMODATION

Juveniles have the right to the same religious accommodation as adults in temporary custody (see the Temporary Custody of Adults Policy).

901.11 USE OF RESTRAINT DEVICES

Juvenile offenders may be handcuffed in accordance with the Handcuffing and Restraints Policy. A juvenile offender may be handcuffed at the Madison County Sheriff's Office when the juvenile presents a heightened risk. However, non-offenders and status offenders should not be handcuffed unless they are combative or threatening.

Other restraints shall only be used after less restrictive measures have failed and with the approval of the Shift Supervisor. Restraints shall only be used so long as it reasonably appears necessary for the juvenile's protection or the protection of others.

Juveniles in restraints shall be kept away from other unrestrained individuals in custody and monitored to protect them from abuse.

901.11.1 PREGNANT JUVENILES

Juveniles who are known to be pregnant should be restrained in accordance with the Handcuffing and Restraints Policy.

901.12 PERSONAL PROPERTY

The personal property of a juvenile shall be processed in the same manner as an adult in temporary custody (see the Temporary Custody of Adults Policy).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

901.13 SECURE CUSTODY

Only juvenile offenders 14 years of age or older may be placed in secure custody. Shift Supervisor approval is required before placing a juvenile offender in secure custody.

Secure custody should only be used for juvenile offenders when there is a reasonable belief that the juvenile is a serious risk of harm to him/herself or others.

Members of this department should not use secure custody for convenience when non-secure custody is, or later becomes, a reasonable option.

When practicable, handcuffing one hand of a juvenile offender to a fixed object while otherwise maintaining the juvenile in non-secure custody should be considered as the method of secure custody. A member must be present at all times to ensure the juvenile's safety while secured to a stationary object.

Generally, juveniles should not be secured to a stationary object for more than 60 minutes. Supervisor approval is required to secure a juvenile to a stationary object for longer than 60 minutes and every 30 minutes thereafter. Supervisor approval should be documented.

901.13.1 LOCKED ENCLOSURES

A thorough inspection of the area shall be conducted before placing a juvenile into the locked enclosure to ensure there are no weapons or contraband and that the area is clean and sanitary. An inspection should be conducted when he/she is released. Any damage noted to the area should be photographed and documented.

The following requirements shall apply:

(a) Anything that could create a security or suicide risk, such as contraband, hazardous items, belts, shoes or shoelaces, and jackets, shall be removed.

(b) The juvenile shall constantly be monitored by an audio/video system during the entire temporary custody.

(c) The juvenile shall have constant auditory access to department members.

(d) The juvenile's initial placement into and removal from a locked enclosure shall be logged.

(e) Unscheduled safety checks by department members shall occur no less than every 15 minutes.

1. All safety checks shall be logged.
2. The safety check should involve questioning the juvenile as to his/her well-being.
3. Juveniles who are sleeping or apparently sleeping should be awakened.
4. Requests or concerns of the juvenile should be logged.

(f) Males and females shall not be placed in the same locked room.

(g) Juvenile offenders should be separated according to severity of the crime (e.g., felony or misdemeanor).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(h) Restrained juveniles shall not be placed in a cell or room with unrestrained juveniles.

901.14 SUICIDE ATTEMPT, DEATH, OR SERIOUS INJURY

The Patrol Division Supervisor will ensure procedures are in place to address any suicide attempt, death, or serious injury of any juvenile held at the Madison County Sheriff's Office. The procedures should include:

(a) Immediate request for emergency medical assistance if appropriate.

(b) Immediate notification of the Shift Supervisor, Sheriff, and Investigation Division Supervisor.

(c) Notification of the parent, guardian, or person standing in loco parentis of the juvenile.

(d) Notification of the appropriate prosecutor.

(e) Notification of the County Attorney.

(f) Notification of the Medical Examiner.

(g) Notification of the juvenile court.

(h) Evidence preservation.

901.15 INTERVIEWING OR INTERROGATING

No interview or interrogation of a juvenile should occur unless the juvenile has the apparent capacity to consent, and does consent, to an interview or interrogation.

901.15.1 PARENTAL NOTIFICATION AND CONTACT

Prior to a custodial interrogation of a juvenile offender taken into custody under Va. Code § 16.1-246(C), (C1), or (D), a deputy shall notify the juvenile’s parent, guardian, or custodian and allow the juvenile to have contact with that parent, guardian, or custodian, unless (Va. Code § 16.1-247.1):

(a) That parent, guardian, or custodian:

1. Is a co-defendant with the juvenile in the offense.
2. Is a suspect for a crime against the juvenile.
3. Cannot be located or refuses contact with the juvenile.

(b) The information sought is necessary to protect persons or property from imminent danger and the questions are limited to that information.

901.15.2 ACCESS TO COUNSEL

If there are valid, substantial reasons a parent or interested adult cannot be present for an interrogation, deputies should ensure before interrogating the juvenile that the juvenile understands the *Miranda* warnings, the consequences of waiving *Miranda* warnings, and that any waiver of the juvenile's rights is made intelligently, knowingly, and voluntarily. A valid waiver will not occur unless the juvenile demonstrates a high degree of intelligence, experience, knowledge, or sophistication. Considerations should also include the juvenile's age, education, and background.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

901.16 RESTRICTION ON FINGERPRINTING AND PHOTOGRAPHING

Fingerprints and photographs shall only be taken if the juvenile is charged with a delinquent act which, if committed by an adult, is required to be reported to Central Criminal Records Exchange (CCRE) pursuant to Va. Code § 19.2-390(A) or if the juvenile is 14 years of age or older and charged with a violent juvenile felony under Va. Code § 16.1-228 (Va. Code § 16.1-299).

Juvenile fingerprint cards and photographs should be separately and securely maintained. Copies of fingerprints shall be filed with the juvenile court on forms provided by the CCRE.

Fingerprint cards and photographs shall be destroyed under the following circumstances (Va. Code § 16.1-299):

(a) If no petition or warrant is filed within 60 days against a juvenile whose fingerprints or photographs have been taken in connection with an alleged violation of law.

(b) Pursuant to a court order.

901.17 TRANSPORTING JUVENILES

No juvenile should be transported with an adult accused of any criminal act (Va. Code § 16.1-254).

901.18 TRAINING

Department members should be trained on and familiar with this policy and any supplemental procedures.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Custodial Searches

902.1 PURPOSE AND SCOPE

This policy provides guidance regarding searches of individuals in custody. Such searches are necessary to eliminate the introduction of contraband, intoxicants or weapons into the Madison County Sheriff's Office facility. Such items can pose a serious risk to the safety and security of department members, individuals in custody, contractors and the public.

Nothing in this policy is intended to prohibit the otherwise lawful collection of evidence from an individual in custody.

902.1.1 DEFINITIONS

Definitions related to this policy include:

Custody search - An in-custody search of an individual and of his/her property, shoes and clothing, including pockets, cuffs and folds on the clothing, to remove all weapons, dangerous items and contraband.

Physical body cavity search - A search that includes a visual inspection and may include a physical intrusion into a body cavity. Body cavity means the stomach or rectal cavity of an individual, and the vagina of a female person.

Strip search - A search that requires an individual to remove or rearrange some or all of his/her clothing to permit a visual inspection of the underclothing, breasts, buttocks, anus or outer genitalia. This includes monitoring an individual who is changing clothes, where his/her underclothing, buttocks, genitalia or female breasts are visible.

902.2 POLICY

All searches shall be conducted with concern for safety, dignity, courtesy, respect for privacy and hygiene, and in compliance with policy and law to protect the rights of those who are subject to any search.

Searches shall not be used for intimidation, harassment, punishment or retaliation.

902.3 FIELD AND TRANSPORTATION SEARCHES

A deputy should conduct a custody search of an individual immediately after his/her arrest, when receiving an individual from the custody of another, and before transporting a person who is in custody in any department vehicle.

Whenever practicable, a custody search should be conducted by a deputy of the same sex as the person being searched. If a deputy of the same sex is not reasonably available, a witnessing deputy should be present during the search.

902.4 SEARCHES AT SHERIFF'S FACILITIES

Custody searches shall be conducted on all individuals in custody, upon entry to the Madison County Sheriff's Office facilities. Except in exigent circumstances, the search should be conducted

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

by a member of the same sex as the individual being searched. If a member of the same sex is not available, a witnessing member must be present during the search.

Custody searches should also be conducted any time an individual in custody enters or re-enters a secure area, or any time it is reasonably believed that a search is necessary to maintain the safety and security of the facility.

902.4.1 PROPERTY

Members shall take reasonable care in handling the property of an individual in custody to avoid discrepancies or losses. Property retained for safekeeping shall be kept in a secure location until the individual is released or transferred.

Some property may not be accepted by a facility or agency that is taking custody of an individual from this department, such as weapons or large items. These items should be retained for safekeeping in accordance with the Property and Evidence Section Policy.

All property shall be inventoried by objective description (this does not include an estimated value). The individual from whom it was taken shall be required to sign the completed inventory. If the individual's signature cannot be obtained, the inventory shall be witnessed by another department member (6 VAC 15-40-1260). The inventory should include the case number, date, time, member's Madison County Sheriff's Office identification number and information regarding how and when the property may be released.

902.4.2 VERIFICATION OF MONEY

All money shall be counted in front of the individual from whom it was received. When possible, the individual shall initial the dollar amount on the inventory. Additionally, all money should be placed in a separate envelope and sealed. Negotiable checks or other instruments and foreign currency should also be sealed in an envelope with the amount indicated but not added to the cash total. All envelopes should clearly indicate the contents on the front. The department member sealing it should place his/her initials across the sealed flap. Should any money be withdrawn or added, the member making such change shall enter the amount below the original entry and initial it. The amount of money in the envelope should always be totaled and written on the outside of the envelope.

902.5 STRIP SEARCHES

No individual in temporary custody at any Madison County Sheriff's Office facility shall be subjected to a strip search unless there is reasonable suspicion based upon specific and articulable facts to believe the individual has a health condition requiring immediate medical attention, or is concealing a weapon or contraband. Factors to be considered in determining reasonable suspicion include but are not limited to:

(a) The detection of an object during a custody search that may be a weapon or contraband and cannot be safely retrieved without a strip search.

(b) Circumstances of a current arrest that specifically indicate the individual may be concealing a weapon or contraband.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1. A felony arrest charge or being under the influence of a controlled substance should not suffice as reasonable suspicion absent other facts.

(c) Custody history (e.g., past possession of contraband while in custody, assaults on department members, escape attempts).

(d) The individual’s actions or demeanor.

(e) Criminal history (i.e., level of experience in a custody setting).

No transgender or intersex individual shall be searched or examined for the sole purpose of determining the individual’s genital status. If the individual’s genital status is unknown, it may be determined during conversations with the person, by reviewing medical records, or as a result of a broader medical examination conducted in private by a medical practitioner (28 CFR 115.115).

A strip search of an individual 17 years of age or under or who is in custody solely for one or more of the following offenses shall only be permitted if a deputy determines there is reasonable cause to believe the individual is concealing a weapon (Va. Code § 19.2-59.1; 6 VAC 15-40-1230):

- Traffic infraction
- Class 3 or Class 4 misdemeanor
- Violation of a city, county, or town ordinance, which is punishable by no more than 30 days in jail

902.5.1 STRIP SEARCH PROCEDURES

Strip searches at Madison County Sheriff's Office facilities shall be conducted as follows (28 CFR 115.115):

(a) Written authorization from the Shift Supervisor shall be obtained prior to the strip search.

(b) All members involved with the strip search shall be of the same sex as the individual being searched, unless the search is conducted by a medical practitioner (Va. Code § 19.2-59.1).

(c) All strip searches shall be conducted in a professional manner under sanitary conditions and in a secure area of privacy so that the search cannot be observed by those not participating in the search. The search shall not be reproduced through a visual or sound recording.

(d) Whenever possible, a second member of the same sex should also be present during the search, for security and as a witness to the finding of evidence.

(e) Members conducting a strip search shall not touch the breasts, buttocks or genitalia of the individual being searched.

(f) The primary member conducting the search shall prepare a written report to include:

1. The facts that led to the decision to perform a strip search.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. The reasons less intrusive methods of searching were not used or were insufficient.
3. The written authorization for the search, obtained from the Shift Supervisor.
4. The name of the individual who was searched.
5. The name and sex of the members who conducted the search.
6. The name, sex and role of any person present during the search.
7. The time and date of the search.
8. The place at which the search was conducted.
9. A list of the items, if any, that were recovered.
10. The facts upon which the member based his/her belief that the individual was concealing a weapon or contraband.

(g) No member should view an individual's private underclothing, buttocks, genitalia or female breasts while that individual is performing bodily functions or changing clothes, unless he/she otherwise qualifies for a strip search. However, if serious hygiene or health issues make it reasonably necessary to assist the individual with a shower or a change of clothes, a supervisor should be contacted to ensure reasonable steps are taken to obtain the individual's consent and/or otherwise protect his/her privacy and dignity.

902.5.2 SPECIAL CIRCUMSTANCE FIELD STRIP SEARCHES

A strip search may be conducted in the field only with Shift Supervisor authorization and only in exceptional circumstances, such as when:

(a) There is probable cause to believe that the individual is concealing a weapon or other dangerous item that cannot be recovered by a more limited search.

(b) There is probable cause to believe that the individual is concealing controlled substances or evidence that cannot be recovered by a more limited search, and there is no reasonable alternative to ensure the individual cannot destroy or ingest the substance during transportation.

These special-circumstance field strip searches shall only be authorized and conducted under the same restrictions as the strip search procedures in this policy, except that the Shift Supervisor authorization does not need to be in writing.

902.6 PHYSICAL BODY CAVITY SEARCH

Physical body cavity searches shall be subject to the following:

(a) No individual shall be subjected to a physical body cavity search without written approval of the Shift Supervisor and only upon a search warrant. A copy of any search warrant and the results of the physical body cavity search shall be included with

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

the related reports and made available, upon request, to the individual or authorized representative (except for those portions of the warrant ordered sealed by a court).

(b) Only medically trained personnel may conduct a physical body cavity search (Va. Code § 19.2-59.1).

(c) Except for the medically trained personnel conducting the search, persons present must be of the same sex as the individual being searched. Only the necessary department members needed to maintain the safety and security of the medical personnel shall be present.

(d) Privacy requirements, including restricted touching of body parts and sanitary condition requirements, are the same as required for a strip search (Va. Code § 19.2-59.1).

(e) All such searches shall be documented, including:

1. The facts that led to the decision to perform a physical body cavity search of the individual.
2. The reasons less intrusive methods of searching were not used or were insufficient.
3. The Shift Supervisor’s approval.
4. A copy of the search warrant.
5. The time, date and location of the search.
6. The medical personnel present.
7. The names, sex and roles of any department members present.
8. Any contraband or weapons discovered by the search.

(f) A copy of the written authorization shall be retained and shall be made available to the individual who was searched or other authorized representative upon request.

902.7 TRAINING

The Training Supervisor shall ensure members have training that includes (28 CFR 115.115):

(a) Conducting searches of cross-gender individuals.

(b) Conducting searches of transgender and intersex individuals.

(c) Conducting searches in a professional and respectful manner, and in the least intrusive manner possible, consistent with security needs.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Prison Rape Elimination

903.1 PURPOSE AND SCOPE

This policy provides guidance for compliance with the Prison Rape Elimination Act of 2003 (PREA) and the implementing regulation that establishes standards (PREA Rule) to prevent, detect and respond to sexual abuse and sexual harassment (28 CFR 115.111).

903.1.1 DEFINITIONS

Definitions related to this policy include:

Intersex - A person whose sexual or reproductive anatomy or chromosomal pattern does not seem to fit typical definitions of male or female. Intersex medical conditions are sometimes referred to as disorders of sex development (28 CFR 115.5).

Sexual abuse - Any of the following acts, if the individual in custody does not consent, is coerced into such act by overt or implied threats of violence, or is unable to consent or refuse:

- Contact between the penis and the vulva or the penis and the anus, including penetration, however slight
- Contact between the mouth and the penis, vulva or anus
- Penetration of the anal or genital opening of another person, however slight, by a hand, finger, object or other instrument
- Any other intentional touching, either directly or through the clothing, of the genitalia, anus, groin, breast, inner thigh or the buttocks of another person, excluding contact incidental to a physical altercation

Sexual abuse also includes abuse by a member of the Department or a contractor, with or without consent of the individual in custody, as follows:

- Contact between the penis and the vulva or the penis and the anus, including penetration, however slight
- Contact between the mouth and the penis, vulva or anus
- Contact between the mouth and any body part where the department member or contractor has the intent to abuse, arouse or gratify sexual desire
- Penetration of the anal or genital opening, however slight, by a hand, finger, object or other instrument, that is unrelated to official duties, or where the department member or contractor has the intent to abuse, arouse or gratify sexual desire
- Any other intentional contact, either directly or through the clothing, of or with the genitalia, anus, groin, breast, inner thigh or the buttocks, that is unrelated to official duties, or where the member or contractor has the intent to abuse, arouse or gratify sexual desire

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

- Any attempt, threat or request by the department member or contractor to engage in the activities described above
- Any display by the department member or contractor of his/her uncovered genitalia, buttocks or breast in the presence of an individual in custody
- Voyeurism by the department member or contractor (28 CFR 115.6)

Sexual harassment - Repeated and unwelcome sexual advances; requests for sexual favors; verbal comments, gestures or actions of a derogatory or offensive sexual nature by one individual in custody that are directed toward another; or repeated verbal comments or gestures of a sexual nature to an individual in custody by a member of the Department or contractor, including demeaning references to gender, sexually suggestive or derogatory comments about body or clothing, or obscene language or gestures (28 CFR 115.6).

Transgender - A person whose gender identity (i.e., internal sense of feeling male or female) is different from the person’s assigned sex at birth (28 CFR 115.5).

903.2 POLICY

The Madison County Sheriff's Office has zero tolerance with regard to all forms of sexual abuse and sexual harassment (28 CFR 115.111). The Department will not tolerate retaliation against any person who reports sexual abuse or sexual harassment, or who cooperates with a sexual abuse or sexual harassment investigation.

The Madison County Sheriff's Office will take immediate action to protect those in its custody who are reasonably believed to be subject to a substantial risk of imminent sexual abuse (28 CFR 115.162).

903.3 PREA COORDINATOR

The Sheriff shall delegate certain responsibilities to a PREA coordinator. The coordinator shall be an upper-level manager appointed by and directly responsible to the Patrol Division Supervisor or the authorized designee. The coordinator must have sufficient time and authority to develop, implement and oversee department efforts to comply with PREA standards (28 CFR 115.111).

The responsibilities of the coordinator shall include, but are not limited to:

(a) Developing and maintaining procedures to comply with the PREA Rule.

(b) Ensuring that any contract for the confinement of individuals in custody includes the requirement to adopt and comply with applicable provisions in PREA and the implementing regulations, including the obligation to provide incident-based and aggregated data, as required in 28 CFR 115.187 (28 CFR 115.112).

(c) Developing a staffing plan to provide adequate levels of staffing and video monitoring, where applicable, in order to protect those in custody from sexual abuse (28 CFR 115.113).

1. This includes documenting deviations and the reasons for deviations from the staffing plan, as well as reviewing the staffing plan a minimum of once per year.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Developing methods for department members to privately report sexual abuse and sexual harassment of individuals in custody (28 CFR 115.151).

(e) Developing a written plan to coordinate response among department members, medical and mental health practitioners, investigators, command staff and other first responders to an incident of sexual abuse (28 CFR 115.165).

(f) Ensuring a protocol is developed for investigating allegations of sexual abuse. The protocol shall include (28 CFR 115.121; 28 CFR 115.122):

1. Evidence collection practices that maximize the potential for obtaining usable physical evidence based on the most recent edition of the U.S. Department of Justice's (DOJ) Office on Violence Against Women publication, "A National Protocol for Sexual Assault Medical Forensic Examinations, Adults/ Adolescents" or a similarly comprehensive and authoritative protocol.
2. A process to ensure a criminal or administrative investigation is completed on all allegations of sexual abuse or sexual harassment.
3. A process to document all referrals to other law enforcement agencies.
4. Access to forensic medical examinations, without financial cost, for all victims of sexual abuse where appropriate. Such examinations shall be performed by Sexual Assault Forensic Examiners (SAFEs) or Sexual Assault Nurse Examiners (SANEs) where possible. If SAFEs or SANEs cannot be made available, the examination can be performed by other qualified medical practitioners. The efforts to provide SAFEs or SANEs shall be documented.
5. In accordance with security needs, provisions to give, to the extent available, individuals in custody access to victim advocacy services if the individual is transported for a forensic examination to an outside hospital that offers such services.

(g) Ensuring that individuals with limited English proficiency and disabilities have an equal opportunity to understand and benefit from efforts to prevent, detect and respond to sexual abuse and sexual harassment. This includes access to appropriate interpreters and written materials in formats or through methods that provide effective communication to those with disabilities (e.g., limited reading skills; intellectual, hearing, speech or vision disabilities) (see the Limited English Proficiency Services and Communications for Persons with Disabilities policies) (28 CFR 115.116).

1. The Department shall not rely on other individuals in custody for assistance except in limited circumstances where an extended delay in obtaining an appropriate interpreter could compromise the individual's safety, the performance of first-response duties under this policy, or the investigation of an individual's allegations of sexual abuse, harassment or retaliation.

(h) Publishing on the department website:

1. Information on how to report sexual abuse and sexual harassment on behalf of an individual in custody (28 CFR 115.154).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. A protocol describing the responsibilities of the Department and any other investigating agency responsible for conducting sexual abuse or sexual harassment investigations (28 CFR 115.122).

(i) Establishing a process that includes the use of a standardized form and set of definitions to ensure accurate, uniform data is collected for every allegation of sexual abuse at facilities under the direct control of this department (28 CFR 115.187).

1. The data collected shall include, at a minimum, the data necessary to answer all questions from the most recent version of the Survey of Sexual Violence, conducted by DOJ, or any subsequent form developed by DOJ and designated for lockups.

2. The data shall be aggregated at least annually.

(j) Ensuring audits are conducted pursuant to 28 CFR 115.401 through 28 CFR 115.405 for all department facilities used to house individuals in custody overnight (28 CFR 115.193).

(k) Ensuring those who work in department facilities where individuals are held in custody are informed of the department zero-tolerance policy regarding sexual abuse and sexual harassment of individuals in custody (28 CFR 115.132).

903.4 REPORTING SEXUAL ABUSE AND HARASSMENT

Individuals in custody may make reports verbally, in writing, privately or anonymously of any of the following (28 CFR 115.151):

- Sexual abuse
- Sexual harassment
- Retaliation by other individuals in custody or department members for reporting sexual abuse or sexual harassment
- Department member neglect or violation of responsibilities that may have contributed to sexual abuse or sexual harassment

Individuals in custody shall be notified of the department zero-tolerance policy regarding sexual abuse and sexual harassment, and of at least one way to report abuse or harassment to a public or private entity that is not part of the Department and that is able to receive and immediately forward a report of sexual abuse or sexual harassment to department supervisors and command staff. This allows the individual to remain anonymous (28 CFR 115.132; 28 CFR 115.151).

903.4.1 MEMBER RESPONSIBILITIES

Department members shall accept reports from individuals in custody and third parties, and shall promptly document all reports (28 CFR 115.151).

All members shall report immediately to the Shift Supervisor any knowledge, suspicion or information regarding:

(a) An incident of sexual abuse or sexual harassment.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Retaliation against the individual or the member who reports any such incident.

(c) Any neglect or violation of responsibilities on the part of any department member that may have contributed to an incident or retaliation (28 CFR 115.161).

No member shall reveal any information related to a sexual abuse report to anyone other than to the extent necessary to make treatment and investigation decisions.

903.4.2 SHIFT SUPERVISOR RESPONSIBILITIES

The Shift Supervisor shall report to Madison County Sheriff's Office designated investigators all allegations of sexual abuse, harassment, retaliation, neglect or violations leading to sexual abuse, harassment or retaliation. This includes third-party and anonymous reports (28 CFR 115.161).

If the alleged victim is under the age of 18 or considered a dependent adult, the Shift Supervisor shall also report the allegation as required under mandatory reporting laws and department policy.

Upon receiving an allegation that an individual in custody was sexually abused while confined at another facility, the Shift Supervisor shall notify the head of that facility or the appropriate office of the agency where the alleged abuse occurred. The notification shall be made as soon as possible but no later than 72 hours after receiving the allegation. The Shift Supervisor shall document such notification (28 CFR 115.163).

If an alleged victim is transferred from the Department to a jail, prison or medical facility, the Shift Supervisor shall, as permitted by law, inform the receiving facility of the incident and the individual's potential need for medical or social services, unless the individual requests otherwise (28 CFR 115.165).

903.5 INVESTIGATIONS

The Department shall promptly, thoroughly and objectively investigate all allegations, including third-party and anonymous reports, of sexual abuse or sexual harassment. Only investigators who have received department-approved special training shall conduct sexual abuse investigations (28 CFR 115.171).

903.5.1 FIRST RESPONDER RESPONSIBILITIES

The responsibilities of the first deputy to respond to a report of sexual abuse or sexual assault shall include, but are not limited to (28 CFR 115.164):

(a) Separating the parties.

(b) Establishing a crime scene to preserve and protect any evidence.

(c) Identifying and securing witnesses until steps can be taken to collect any evidence.

(d) Requesting that the alleged victim and suspect not take any actions that could destroy physical evidence, including, as appropriate, washing, brushing teeth, changing clothes, urinating, defecating, smoking, drinking or eating if the abuse occurred within a time period that still allows for the collection of physical evidence.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

If the first responder is not a deputy, he/she shall request that the alleged victim not take any actions that could destroy physical evidence and should then notify a deputy (28 CFR 115.164).

903.5.2 INVESTIGATOR RESPONSIBILITIES

The responsibilities of investigators shall include, but are not limited to (28 CFR 115.171):

(a) Gathering and preserving direct and circumstantial evidence, including any available physical and biological evidence and any available electronic monitoring data.

(b) Interviewing alleged victims, suspects and witnesses.

(c) Reviewing any prior complaints and reports of sexual abuse involving the suspect.

(d) Conducting compelled interviews only after consulting with prosecutors as to whether compelled interviews may be an obstacle for subsequent criminal prosecution.

(e) Assessing the credibility of the alleged victim, suspect or witness on an individual basis and not by the person’s status as an individual in custody or a member of the Madison County Sheriff's Office.

(f) Documenting in written reports a description of physical, testimonial, documentary and other evidence, the reasoning behind any credibility assessments, and investigative facts and findings.

(g) Referring allegations of conduct that may be criminal to the Commonwealth Attorney for possible prosecution, including any time there is probable cause to believe an individual in custody sexually abused another individual in custody at the department facility (28 CFR 115.178).

(h) Cooperating with outside investigators and remaining informed about the progress of any outside investigation.

903.5.3 ADMINISTRATIVE INVESTIGATIONS

Administrative investigations shall include an effort to determine whether department member actions or failures to act contributed to the abuse. The departure of the alleged abuser or victim from the employment or control of this department shall not be used as a basis for terminating an investigation (28 CFR 115.171).

903.5.4 SEXUAL ASSAULT AND SEXUAL ABUSE VICTIMS

No individual in custody who alleges sexual abuse shall be required to submit to a polygraph examination or other truth telling device as a condition for proceeding with the investigation of such an allegation (28 CFR 115.171(e)).

Victims of sexual abuse shall receive timely, unimpeded access to emergency medical treatment. Treatment services shall be provided to the victim without financial cost and regardless of whether the victim names the abuser or cooperates with any investigation arising out of the incident (28 CFR 115.182).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

903.5.5 CONCLUSIONS AND FINDINGS

All completed investigations shall be forwarded to the Sheriff, or if the allegations may reasonably involve the Sheriff, to the County Administrator. The Sheriff or County Administrator shall review the investigation and determine whether any allegations of sexual abuse or sexual harassment have been substantiated by a preponderance of the evidence (28 CFR 115.172).

All department members shall be subject to disciplinary sanctions up to and including termination for violating this policy. Termination shall be the presumptive disciplinary sanction for members who have engaged in sexual abuse. All discipline shall be commensurate with the nature and circumstances of the acts committed, the member's disciplinary history and the sanctions imposed for comparable offenses by other members with similar histories (28 CFR 115.176).

All terminations for violations of this policy, or resignations by members who would have been terminated if not for their resignation, shall be criminally investigated unless the activity was clearly not criminal and reported to any relevant licensing body (28 CFR 115.176).

Any contractor who engages in sexual abuse shall be prohibited from contact with individuals in custody and reported to any relevant licensing bodies (28 CFR 115.177). The Sheriff shall take appropriate remedial measures and consider whether to prohibit further contact with individuals in custody by a contractor.

903.6 RETALIATION PROHIBITED

All individuals in custody and department members who report sexual abuse or sexual harassment or who cooperate with sexual abuse or sexual harassment investigations shall be protected from retaliation (28 CFR 115.167). If any other person who cooperates with an investigation expresses a fear of retaliation, appropriate measures shall be taken to protect that person.

The Shift Supervisor or the authorized designee shall employ multiple protection measures, such as housing changes or transfers for victims or abusers, removal of alleged abusers from contact with victims, and emotional support services for individuals in custody or members who fear retaliation for reporting sexual abuse or sexual harassment or for cooperating with investigations.

A member of the Department shall be identified by the Shift Supervisor or the authorized designee to monitor the conduct and treatment of individuals in custody or members who have reported sexual abuse, and of those who were reported to have suffered sexual abuse. The member shall act promptly to remedy any such retaliation. In the case of individuals in custody, such monitoring shall also include periodic safety checks.

903.7 REVIEWS AND AUDITS

903.7.1 INCIDENT REVIEWS

An incident review shall be conducted at the conclusion of every sexual abuse investigation, unless the allegation has been determined to be unfounded. The review should occur within 30 days of the conclusion of the investigation. The review team shall include command staff and seek input from supervisors and investigators (28 CFR 115.186).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

The review shall (28 CFR 115.186):

(a) Consider whether the allegation or investigation indicates a need to change policy or practice to better prevent, detect or respond to sexual abuse.

(b) Consider whether the incident or allegation was motivated by race; ethnicity; gender identity; lesbian, gay, bisexual, transgender or intersex identification, status or perceived status; gang affiliation; or other group dynamics at the department facility.

(c) Examine the area in the facility where the incident allegedly occurred to assess whether physical barriers in the area may enable abuse.

(d) Assess the adequacy of staffing levels in that area during different shifts.

(e) Assess whether monitoring technology should be deployed or augmented to supplement supervision by department members.

The review team shall prepare a report of its findings, including any determinations made pursuant to this section and any recommendations for improvement. The report shall be submitted to the Sheriff and the PREA coordinator. The Sheriff or the authorized designee shall implement the recommendations for improvement or shall document the reasons for not doing so (28 CFR 115.186).

903.7.2 DATA REVIEWS

The PREA coordinator shall conduct an annual review of collected and aggregated incident-based sexual abuse data. The review should include, as needed, data from incident-based documents, including reports, investigation files, and sexual abuse incident reviews (28 CFR 115.187).

The purpose of these reviews is to assess and improve the effectiveness of sexual abuse prevention, detection and response policies, practices, and training. An annual report shall be prepared that includes (28 CFR 115.188):

(a) Identification of any potential problem areas.

(b) Identification of any corrective actions taken.

(c) Recommendations for any additional corrective actions.

(d) A comparison of the current year's data and corrective actions with those from prior years.

(e) An assessment of the progress in addressing sexual abuse.

The report shall be approved by the Sheriff and made readily available to the public through the department website. Material may be redacted from the reports when publication would present a clear and specific threat to the safety and security of the facility. However, the nature of the redacted material shall be indicated.

All aggregated sexual abuse data from department facilities and private facilities with which it contracts shall be made readily available to the public at least annually. Before making aggregated sexual abuse data publicly available, all personal identifiers shall be removed (28 CFR 115.189).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

903.8 RECORDS

The Madison County Sheriff's Office shall retain all written reports from administrative and criminal investigations pursuant to this policy for as long as the alleged abuser is in custody or is a member of the Department, plus five years (28 CFR 115.171).

All other data collected pursuant to this policy shall be securely retained for at least 10 years after the date of the initial collection unless federal, state or local law requires otherwise (28 CFR 115.189).

903.9 TRAINING

All department members and contractors who may have contact with individuals in custody shall receive department-approved training on the prevention and detection of sexual abuse and sexual harassment within the department facility.

(a) The Training Supervisor shall be responsible for developing and administering this training as appropriate, covering at a minimum (28 CFR 115.131):

1. The department zero-tolerance policy and the right of individuals in custody to be free from sexual abuse and sexual harassment and from retaliation for reporting sexual abuse or harassment.
2. The dynamics of sexual abuse and harassment in confinement settings, including which individuals in custody are most vulnerable.
3. The right of individuals in custody and department members to be free from sexual abuse and sexual harassment, and from retaliation for reporting sexual abuse or harassment.
4. Detecting and responding to signs of threatened and actual abuse.
5. Communicating effectively and professionally with all individuals in custody.
6. Compliance with relevant laws related to mandatory reporting of sexual abuse to outside authorities.

(b) Investigators assigned to sexual abuse investigations shall also receive training in conducting such investigations in confinement settings. Training should include (28 CFR 115.134):

1. Techniques for interviewing sexual abuse victims.
2. Proper use of *Miranda* and *Garrity* warnings.
3. Sexual abuse evidence collection in confinement settings.
4. Criteria and evidence required to substantiate a case for administrative action or prosecution referral.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Prison Rape Elimination

The Training Supervisor shall maintain documentation that department members, contractors and investigators have completed required training and that they understand the training. This understanding shall be documented through individual signature or electronic verification.

All current department members who may have contact with individuals in custody shall be trained within one year of the effective date of the PREA standards. The Department shall provide annual refresher information to all such members to ensure that they understand the current sexual abuse and sexual harassment policies and procedures.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Chapter 10 - Personnel

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Recruitment and Selection

1000.1 PURPOSE AND SCOPE

This policy provides a framework for employee recruiting efforts and identifying job-related standards for the selection process. This policy supplements the rules that govern employment practices for the Madison County Sheriff's Office and that are promulgated and maintained by the Human Resources Department.

1000.2 POLICY

In accordance with applicable federal, state, and local law, the Madison County Sheriff's Office provides equal opportunities for applicants and employees regardless of actual or perceived race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, age, disability, pregnancy, genetic information, veteran status, marital status, and any other classification or status protected by law. The Department does not show partiality or grant any special status to any applicant, employee, or group of employees unless otherwise required by law.

The Department will recruit and hire only those individuals who demonstrate a commitment to service and who possess the traits and characteristics that reflect personal integrity and high ethical standards.

1000.3 RECRUITMENT

The Administration Division Supervisor should employ a comprehensive recruitment and selection strategy to recruit and select employees from a qualified and diverse pool of candidates.

The strategy should include:

(a) Identification of racially and culturally diverse target markets.

(b) Use of marketing strategies to target diverse applicant pools.

(c) Expanded use of technology and maintenance of a strong internet presence. This may include an interactive department website and the use of department-managed social networking sites, if resources permit.

(d) Expanded outreach through partnerships with media, community groups, citizen academies, local colleges, universities, and the military.

(e) Employee referral and recruitment incentive programs.

(f) Consideration of shared or collaborative regional testing processes.

The Administration Division Supervisor shall avoid advertising, recruiting, and screening practices that tend to stereotype, focus on homogeneous applicant pools, or screen applicants in a discriminatory manner.

The Department should strive to facilitate and expedite the screening and testing process, and should periodically inform each candidate of his/her status in the recruiting process.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1000.4 SELECTION PROCESS

The Department shall actively strive to identify a diverse group of candidates who have in some manner distinguished themselves as being outstanding prospects. Minimally, the Department should employ a comprehensive screening, background investigation, and selection process that assesses cognitive and physical abilities and includes review and verification of the following:

(a) A comprehensive application for employment (including previous employment, references, current and prior addresses, education, and military record)

(b) Driving record

(c) Reference checks

(d) Employment eligibility, including U.S. Citizenship and Immigration Services (USCIS) Employment Eligibility Verification Form I-9 and acceptable identity and employment authorization documents. This required documentation should not be requested until a candidate is hired. This does not prohibit obtaining documents required for other purposes.

(e) Information obtained from public internet sites

(f) Financial history consistent with the Fair Credit Reporting Act (FCRA) (15 USC § 1681 et seq.)

(g) Local, state, and federal criminal history record checks (Va. Code § 15.2-1705; Va. Code § 15.2-1503.1; Va. Code § 15.2-1505.1; Va. Code § 19.2-389)

(h) Polygraph or voice stress analyzer examination (when legally permissible)

(i) Medical and psychological examination (may only be given after a conditional offer of employment) (Va. Code § 15.2-1705)

(j) Review board or selection committee assessment

1000.4.1 VETERAN PREFERENCE

The Department will provide veteran preference points as required (Va. Code § 15.2-1509).

1000.4.2 DISABILITY PREFERENCE

The Department will provide preference to candidates with a disability who meet the minimum qualifications for employment pursuant to Va. Code § 15.2-1509.

1000.5 BACKGROUND INVESTIGATION

Every candidate shall undergo a thorough background investigation to verify his/her personal integrity and high ethical standards, and to identify any past behavior that may be indicative of the candidate's unsuitability to perform duties relevant to the operation of the Madison County Sheriff's Office.

1000.5.1 NOTICES

Background investigators shall ensure that investigations are conducted and notices provided in accordance with the requirements of the FCRA (15 USC § 1681d).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1000.5.1 STATE NOTICES

If required, the Department shall notify the candidate of the information appearing in his/her criminal history record if the information is a basis for an adverse employment determination (Va. Code § 15.2-1503.1).

1000.5.2 REVIEW OF SOCIAL MEDIA SITES

Due to the potential for accessing unsubstantiated, private or protected information, the Administration Division Supervisor shall not require candidates to provide passwords, account information or access to password-protected social media accounts (Va. Code § 40.1-28.7:5).

The Administration Division Supervisor should consider utilizing the services of an appropriately trained and experienced third party to conduct open source, internet-based searches and/or review information from social media sites to ensure that:

(a) The legal rights of candidates are protected.

(b) Material and information to be considered are verified, accurate and validated.

(c) The Department fully complies with applicable privacy protections and local, state and federal law.

Regardless of whether a third party is used, the Administration Division Supervisor should ensure that potentially impermissible information is not available to any person involved in the candidate selection process.

1000.5.3 DOCUMENTING AND REPORTING

The background investigator shall summarize the results of the background investigation in a report that includes sufficient information to allow the reviewing authority to decide whether to extend a conditional offer of employment. The report shall not include any information that is prohibited from use, including that from social media sites, in making employment decisions. The report and all supporting documentation shall be included in the candidate’s background investigation file.

1000.5.4 RECORDS RETENTION

The background report and all supporting documentation shall be maintained in accordance with the established records retention schedule.

1000.5.5 ADDITIONAL REQUIREMENTS

The Department shall not request, require, solicit, or administer a genetic test to any applicant as a condition of employment (Va. Code § 40.1-28.7:1).

For all candidates previously employed as a deputy by a law enforcement agency or jail, the Department shall request from any such agencies information related to prior arrests, prosecutions, criminal conduct, excessive use of force, official misconduct, civil suits, or adverse employment actions as required by Va. Code § 15.2-1705, and no candidate may begin employment as a deputy prior to the department’s receipt of that information (Va. Code §

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

15.2-1705). The Department shall request that the candidate complete a waiver or release authorizing the request for this information (Va. Code § 15.2-1705).

1000.6 DISQUALIFICATION GUIDELINES

As a general rule, performance indicators and candidate information and records shall be evaluated by considering the candidate as a whole, and taking into consideration the following (Va. Code § 15.2-1505.1):

- Age at the time the behavior occurred
- Passage of time
- Patterns of past behavior
- Severity of behavior
- Probable consequences if past behavior is repeated or made public
- Likelihood of recurrence
- Relevance of past behavior to public safety employment
- Aggravating and mitigating factors
- Other relevant considerations

A candidate’s qualifications will be assessed on a case-by-case basis, using a totality-of-the-circumstances framework.

1000.7 EMPLOYMENT STANDARDS

All candidates shall meet the minimum standards required by state law. Candidates will be evaluated based on merit, ability, competence, and experience, in accordance with the high standards of integrity and ethics valued by the Department and the community.

Validated, job-related, and nondiscriminatory employment standards shall be established for each job classification and shall minimally identify the training, abilities, knowledge, and skills required to perform the position's essential duties in a satisfactory manner. Each standard should include performance indicators for candidate evaluation and shall be conducted in a uniform manner. The Human Resources Department should maintain validated standards for all positions.

1000.7.1 STANDARDS FOR DEPUTIES

Candidates shall meet minimum standards established by Virginia law, including those required in Va. Code § 15.2-1705:

(a) Be a citizen of the United States

(b) Pass a background investigation including fingerprint-based criminal history records inquiries to both the Central Criminal Records Exchange and the Federal Bureau of Investigation

(c) Possess a high school education or have passed a high school equivalency examination approved by the Board of Education

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Possess a valid driver's license if required by the duties of office to operate a motor vehicle

(e) Pass a physical examination, subsequent to a conditional offer of employment, conducted under the supervision of a licensed physician

(f) Be at least 21 years of age

(g) Not have been convicted of or pled guilty or no contest to a felony or any offense that would be a felony if committed in the Commonwealth

(h) Not have produced a positive result on a pre-employment drug screening, if such screening is required by the Department, where the positive result cannot be explained to the Sheriff's satisfaction

(i) Not have been convicted of or pled guilty or no contest to:

1. Any misdemeanor involving moral turpitude, including but not limited to petit larceny under Va. Code § 18.2-96, or any offense involving moral turpitude that would be a misdemeanor if committed in the Commonwealth
2. Any misdemeanor sex offense in the Commonwealth, another state, or the United States, including but not limited to sexual battery under Va. Code § 18.2-67.4 or consensual sexual intercourse with a minor 15 years of age or older under clause (ii) of Va. Code § 18.2-371
3. Domestic assault under Va. Code § 18.2-57.2 or any offense that would be domestic assault under the laws of another state or the United States

The Sheriff maintains the right to request a waiver and establish department requirements for certain positions when such requirements are determined to be necessary to perform the duties of the position.

1000.8 PROBATIONARY PERIODS

The Administration Division Supervisor should coordinate with the Madison County, Virginia Human Resources Department to identify positions subject to probationary periods and procedures for:

(a) Appraising performance during probation.

(b) Assessing the level of performance required to complete probation.

(c) Extending probation.

(d) Documenting successful or unsuccessful completion of probation.

1000.9 TRAINING

All members involved in conducting the selection process shall have department-approved training in the particular tasks being performed.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Performance Evaluations

1001.1 PURPOSE AND SCOPE

This policy provides guidelines for the Madison County Sheriff's Office performance evaluation system.

1001.2 POLICY

The Madison County Sheriff's Office shall use a performance evaluation system to measure, document, and recognize work performance. The performance evaluation will serve as an objective guide for the recognition of good work and the development of a process for improvement.

The Department evaluates employees in a non-discriminatory manner based upon job-related factors specific to the employee’s position, without regard to actual or perceived race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, age, disability, pregnancy, genetic information, veteran status, marital status, and any other classification or status protected by law.

1001.3 TYPES OF EVALUATIONS

The Department shall use the following types of evaluations:

Regular - An evaluation completed annually by the employee's Division supervisor.

When an employee is promoted or transfers to a different assignment in the middle of an evaluation period, the evaluation should be completed by the current supervisor with input from the previous supervisor.

Special - An evaluation that may be completed at any time the supervisor and Division Supervisor or the authorized designee determine an evaluation is necessary to address less than standard performance. The evaluation may include a plan for follow-up action (e.g., performance improvement plan (PIP), remedial training, retraining).

1001.3.1 RATINGS

When completing an evaluation, the supervisor will identify the rating category that best describes the employee's performance. The definition of each rating category is as follows:

Outstanding - Performance is well beyond that required for the position. It is exceptional performance, definitely superior or extraordinary.

Exceeds standards - Performance is better than demonstrated by a competent employee. It is performance superior to what is required, but is not of such nature to warrant a rating of outstanding.

Meets standards - Performance of a competent employee. It is satisfactory performance that meets the standards required of the position.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Needs improvement - Performance is less than the standards required of the position. A needs improvement rating shall be thoroughly discussed with the employee.

Unsatisfactory - Performance is inferior to the standards required of the position. It is inadequate or undesirable performance that cannot be allowed to continue.

Supervisor comments may be included in the evaluation to document the employee's strengths, weaknesses and requirements for improvement. Any job dimension rating marked as unsatisfactory or outstanding shall be substantiated with supervisor comments.

1001.3.2 PERFORMANCE IMPROVEMENT PLAN

Employees who receive an unsatisfactory rating may be subject to a PIP. The PIP shall delineate areas that need improvement, any improvement measures and a timetable in which to demonstrate improvement. The issuing supervisor shall meet with the employee to review his/her performance and the status of the PIP at least monthly.

1001.4 EVALUATION PROCESS

Supervisors should meet with the employees they supervise at the beginning of the evaluation period to discuss expectations and establish performance standards. Each supervisor should discuss the tasks of the position, standards of expected performance and the evaluation criteria with each employee.

Performance evaluations cover a specific period and should be based upon documented performance dimensions that are applicable to the duties and authorities granted to the employee during that period. Evaluations should be completed by each employee's immediate supervisor. Other supervisors directly familiar with the employee's performance during the rating period should be consulted by the evaluating supervisor for input.

Assessment of an employee's job performance is an ongoing process. Continued coaching and feedback provides supervisors and employees with opportunities to correct performance issues as they arise and to acknowledge good work. Periodic discussions with the employee during the course of the evaluation period are encouraged. Supervisors should document all discussions in the prescribed manner.

Non-probationary employees demonstrating substandard performance shall be notified in writing as soon as possible in order to have an opportunity to remediate the issues. Such notification should occur at the earliest opportunity, with the goal being a minimum of 90 days written notice prior to the end of the evaluation period.

All supervisors shall receive training on performance evaluations within one year of a supervisory appointment.

See attachment: Employee Performance Evaluation.pdf

See attachment: Supervisor Supplemental Eval.pdf

See attachment: Harassment and Discrimination Acknowlegment.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1001.5 EVALUATION FREQUENCY

Supervisors shall ensure that all employees they supervise are evaluated at least once every year on the anniversary of the employee's date of appointment or hire.

Those employees who are required to successfully complete a probationary period should be evaluated monthly.

1001.6 EVALUATION INTERVIEW

When the supervisor has completed his/her evaluation, a private discussion of the evaluation should be scheduled with the employee. The supervisor should discuss the evaluation ratings and respond to any questions the employee may have. The supervisor should provide relevant counseling regarding advancement, specialty positions and training opportunities. Any performance areas in need of improvement and goals for reaching the expected level of performance should be identified and discussed. If the employee has reasonable objections to any of the ratings, the supervisor may make appropriate adjustments to the evaluation. The reason for such adjustments shall be documented.

Employees may write comments in an identified section of the evaluation. The supervisor and employee will sign and date the evaluation.

1001.6.1 DISCRIMINATORY HARASSMENT FORM

At the time of each employee's annual evaluation, the supervisor shall provide access to and require the employee to read the Madison County Sheriff's Office Discriminatory Harassment Policy. The supervisor shall give the employee a form to be completed and returned that acknowledges the following:

(a) The employee understands the harassment and discrimination policies.

(b) The employee has had all questions regarding the policies sufficiently addressed.

(c) The employee knows how to report alleged harassment and discrimination policy violations.

(d) Whether the employee has been the subject of, or witness to, any unreported conduct that may violate the discrimination or harassment policies.

The completed form should be returned to the supervisor (or other authorized individual if the employee is uncomfortable returning the form to the presenting supervisor) within one week. If the employee has expressed any questions or concerns, the receiving supervisor or other authorized individual shall ensure that appropriate follow-up action is taken.

1001.7 APPEAL

An employee who disagrees with his/her evaluation may provide a formal written response that will be attached to the evaluation, or may request an appeal.

To request an appeal, the employee shall forward a written memorandum within three days to the evaluating supervisor's Division Supervisor or the authorized designee. The memorandum shall

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

identify the specific basis for the appeal and include any relevant information for the reviewer to consider.

1001.8 CHAIN OF REVIEW

The signed performance evaluation and any employee attachment should be forwarded to the evaluating supervisor’s Division Supervisor or the authorized designee. The Division Supervisor or the authorized designee shall review the evaluation for fairness, impartiality, uniformity and consistency, and shall consider any written response or appeal made by the employee.

The Division Supervisor or the authorized designee should evaluate the supervisor on the quality of ratings given.

1001.9 RETENTION AND DISTRIBUTION

The original performance evaluation and any original correspondence related to an appeal shall be maintained by the Department in accordance with the Personnel Records Policy.

A copy of the evaluation and any documentation of a related appeal shall be provided to the employee and also forwarded to the Sheriff.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Special Assignments and Promotions

1002.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for promotions and for making special assignments within the Madison County Sheriff's Office.

1002.2 POLICY

The Madison County Sheriff's Office determines assignments and promotions in a nondiscriminatory manner based upon job-related factors and candidate skills and qualifications. Assignments and promotions are made by the Sheriff.

1002.3 SPECIAL ASSIGNMENT POSITIONS

The following positions are considered special assignments and not promotions:

(a) Crisis Response Unit member

(b) Investigator

(c) Canine handler

(d) Accident investigator

(e) Field Training Officer

(f) Community Relations/Training Officer

(g) School Resource and/or Drug Abuse Resistance Education (D.A.R.E.) deputy

(h) Court Officer

1002.3.1 GENERAL REQUIREMENTS

The following requirements should be considered when selecting a candidate for a special assignment:

(a) Two years of relevant experience

(b) Off probation

(c) Possession of or ability to obtain any certification required by the Virginia Department of Criminal Justice Services or law

(d) Exceptional skills, experience or abilities related to the special assignment

1002.3.2 EVALUATION CRITERIA

The following criteria will be used in evaluating candidates for a special assignment:

(a) Presents a professional, neat appearance.

(b) Maintains a physical condition that aids in his/her performance.

(c) Expressed an interest in the assignment.

(d) Demonstrates the following traits:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1. Emotional stability and maturity
2. Stress tolerance
3. Sound judgment and decision-making
4. Personal integrity and ethical conduct
5. Leadership skills
6. Initiative
7. Adaptability and flexibility
8. Ability to conform to department goals and objectives in a positive manner

1002.3.3 SELECTION PROCESS
The selection process for special assignments will include an administrative evaluation as determined by the Sheriff to include:

(a) Supervisor recommendations - Each supervisor who has supervised or otherwise been involved with the candidate will submit a recommendation.
    1. The supervisor recommendations will be submitted to the Division Supervisor for whom the candidate will work.

(b) Division Supervisor interview - The Division Supervisor will schedule interviews with each candidate.
    1. Based on supervisor recommendations and those of the Division Supervisor after the interview, the Division Supervisor will submit his/her recommendations to the Sheriff.

(c) Assignment by the Sheriff.

The selection process for all special assignment positions may be waived for temporary assignments, emergency situations, training and at the discretion of the Sheriff.

1002.3.4 COURTROOM SECURITY ASSIGNMENT
Upon selection of a courtroom security detail, the Sheriff or the authorized designee shall provide a list of designated deputies to the Director of the Virginia Department of Criminal Justice Services (Va. Code § 53.1-120).

1002.4 PROMOTIONAL REQUIREMENTS
Requirements and information regarding any promotional process may be obtained by contacting the Sheriff's Office Administration.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Anti-Retaliation

1003.1 PURPOSE AND SCOPE

This policy prohibits retaliation against members who identify workplace issues, such as fraud, waste, abuse of authority, gross mismanagement or any inappropriate conduct or practices, including violations that may pose a threat to the health, safety or well-being of members.

This policy does not prohibit actions taken for nondiscriminatory or non-retaliatory reasons, such as discipline for cause.

These guidelines are intended to supplement and not limit members' access to other applicable remedies. Nothing in this policy shall diminish the rights or remedies of a member pursuant to any applicable federal law, provision of the U.S. Constitution, state and local law, ordinance or County rule or policy.

1003.2 POLICY

The Madison County Sheriff's Office has a zero tolerance for retaliation and is committed to taking reasonable steps to protect from retaliation members who, in good faith, engage in permitted behavior or who report or participate in the reporting or investigation of workplace issues. All complaints of retaliation will be taken seriously and will be promptly and appropriately investigated.

1003.3 RETALIATION PROHIBITED

No member may retaliate against any person for engaging in lawful or otherwise permitted behavior; for opposing a practice believed to be unlawful, unethical, discriminatory, or retaliatory; for reporting or making a complaint under this policy; or for participating in any investigation related to a complaint under this or any other policy.

Retaliation includes any adverse action or conduct including but not limited to:

- Refusing to hire or denying a promotion.
- Extending the probationary period.
- Unjustified reassignment of duties or change of work schedule.
- Real or implied threats or other forms of intimidation to dissuade the reporting of wrongdoing or filing of a complaint, or as a consequence of having reported or participated in protected activity.
- Taking unwarranted disciplinary action.
- Spreading rumors about the person filing the complaint or about the alleged wrongdoing.
- Shunning or unreasonably avoiding a person because he/she has engaged in protected activity.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1003.4 COMPLAINTS OF RETALIATION

Any member who feels he/she has been retaliated against in violation of this policy should promptly report the matter to any supervisor, command staff member, or the Sheriff.

Members shall act in good faith, not engage in unwarranted reporting of trivial or minor deviations or transgressions, and make reasonable efforts to verify facts before making any complaint in order to avoid baseless allegations. Members shall not report or state an intention to report information or an allegation knowing it to be false or with willful or reckless disregard for the truth or falsity of the information, or otherwise act in bad faith.

Investigations are generally more effective when the identity of the reporting member is known, thereby allowing investigators to obtain additional information from the reporting member. However, complaints may be made anonymously. All reasonable efforts shall be made to protect the reporting member's identity. However, confidential information may be disclosed to the extent required by law or to the degree necessary to conduct an adequate investigation and make a determination regarding a complaint. In some situations, the investigative process may not be complete unless the source of the information and a statement by the member is part of the investigative process.

1003.5 SUPERVISOR RESPONSIBILITIES

Supervisors are expected to remain familiar with this policy and ensure that members under their command are aware of its provisions.

The responsibilities of supervisors include, but are not limited to:

(a) Ensuring complaints of retaliation are investigated as provided in the Personnel Complaints Policy.

(b) Receiving all complaints in a fair and impartial manner.

(c) Documenting the complaint and any steps taken to resolve the problem.

(d) Acknowledging receipt of the complaint, notifying the Sheriff via the chain of command and explaining to the member how the complaint will be handled.

(e) Taking appropriate and reasonable steps to mitigate any further violations of this policy.

(f) Monitoring the work environment to ensure that any member making a complaint is not subjected to further retaliation.

(g) Periodic follow-up with the complainant to ensure that retaliation is not continuing.

(h) Not interfering with or denying the right of a member to make any complaint.

(i) Taking reasonable steps to accommodate requests for assignment or schedule changes made by a member who may be the target of retaliation if it would likely mitigate the potential for further violations of this policy.

1003.6 COMMAND STAFF RESPONSIBILITIES

The Sheriff should communicate to all supervisors the prohibition against retaliation.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Command staff shall treat all complaints as serious matters and shall ensure that prompt actions take place including, but not limited to:

(a) Communicating to all members the prohibition against retaliation.

(b) The timely review of complaint investigations.

(c) Remediation of any inappropriate conduct or condition and instituting measures to eliminate or minimize the likelihood of recurrence.

(d) The timely communication of the outcome to the complainant.

1003.7 WHISTLE-BLOWING

State law protects:

(a) Members from retaliation for the reporting or intended reporting of violations of law or of the misuse, destruction, waste, or loss of public funds or resources (Va. Code § 2.2-3010.1; Va. Code § 2.2-3011; Va. Code § 40.1-27.3; 1 VAC 42-30-10 et seq.).

(b) Employees when exercising certain rights to report safety or health issues or to otherwise comment regarding matters of public concern or matters of interest to the community as a whole (Va. Code § 15.2-1512.4; Va. Code § 40.1-51.2:1).

(c) Employees from retaliation regarding the terms and conditions of employment for (Va. Code § 40.1-27.3):

1. Providing information or testimony, or participating upon request, in any investigation, hearing, or inquiry by law enforcement or a governmental body.

2. Refusing to engage in a criminal act that would subject the employee to criminal liability.

3. Refusing to carry out an order that would result in a violation of law, provided the employee informs the employer of the reason for refusal.

Members who believe they have been the subject of retaliation for engaging in such protected behaviors should promptly report it to a supervisor. Supervisors should refer the complaint to the Internal Affairs Unit for investigation pursuant to the Personnel Complaints Policy.

1003.7.1 INFORMATION DISTRIBUTION

The Department shall post notices and take other reasonable measures to make sure employees are informed of the protections and obligations of the Virginia Fraud and Abuse Whistle Blower Protection Act (Va. Code § 2.2-3013).

1003.8 RECORDS RETENTION AND RELEASE

The Records Manager shall ensure that documentation of investigations is maintained in accordance with the established records retention schedules.

1003.9 TRAINING

This policy should be reviewed with each new member.

All members should receive periodic refresher training on the requirements of this policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Reporting of Arrests, Convictions and Court Orders

1004.1 PURPOSE AND SCOPE

The purpose of this policy is to describe the notification requirements and procedures that members must follow when certain arrests, convictions and court orders restrict their ability to perform the official duties and responsibilities of the Madison County Sheriff's Office. This policy will also describe the notification requirements and procedures that certain retired deputies must follow when an arrest, conviction or court order disqualifies them from possessing a firearm.

1004.2 POLICY

The Madison County Sheriff's Office requires disclosure of member arrests, convictions and certain court orders to maintain the high standards, ethics and integrity in its workforce, and to ensure compatibility with the duties and responsibilities of the Department.

1004.3 DOMESTIC OR FAMILY VIOLENCE CONVICTIONS AND COURT ORDERS

Federal and Virginia law prohibit individuals convicted of certain offenses and individuals subject to certain court orders from lawfully possessing firearms. Such convictions and court orders often involve allegations of the use or attempted use of force, or threatened use of a weapon on any individual in a domestic relationship (e.g., spouse, cohabitant, parent, child) (18 USC § 922; Va. Code § 18.2-308.2).

All members and retired deputies with identification cards issued by the Department are responsible for ensuring that they have not been disqualified from possessing firearms by any such conviction or court order, and shall promptly report any such conviction or court order to a supervisor, as provided in this policy.

1004.4 OTHER CRIMINAL CONVICTIONS AND COURT ORDERS

While legal restrictions may or may not be imposed by statute or by the courts upon conviction of any criminal offense, criminal conduct by members of this department may be inherently in conflict with law enforcement duties and the public trust, and shall be reported as provided in this policy.

Virginia law prohibits individuals convicted of or pleading guilty or no contest to a felony and certain misdemeanors from becoming a deputy (Va. Code § 15.2-1705).

1004.5 REPORTING

All members and all retired deputies with identification cards issued by the Department shall immediately notify their supervisors (retired deputies should immediately notify the Shift Supervisor or the Sheriff) in writing of any past or current criminal detention, arrest, charge or conviction in any state or foreign country, regardless of whether the matter was dropped or rejected, is currently pending or is on appeal, and regardless of the penalty or sentence, if any.

All members and all retired deputies with identification cards issued by the Department shall immediately notify their supervisors (retired deputies should immediately notify the Shift

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Supervisor or the Sheriff) in writing if they become the subject of a domestic or family violence-related order or any court order that prevents the member or retired deputy from possessing a firearm or requires suspension or revocation of applicable Virginia Department of Criminal Justice Services (DCJS) certification.

Any member whose criminal arrest, conviction or court order restricts or prohibits that member from fully and properly performing his/her duties, including carrying a firearm, may be disciplined. This includes, but is not limited to, being placed on administrative leave, reassignment and/or termination. Any effort to remove such disqualification or restriction shall remain entirely the responsibility of the member, on his/her own time and at his/her own expense.

Any employee failing to provide prompt written notice pursuant to this policy shall be subject to discipline, up to and including termination.

Retired deputies may have their identification cards rescinded or modified, as may be appropriate (see the Retired Officer Identification Card Policy).

1004.5.1 NOTIFICATION REQUIREMENTS

The Administration Division Supervisor shall submit, in writing, the proper notice to the DCJS within 48 hours of becoming aware that a deputy has (Va. Code § 15.2-1707):

(a) Failed to maintain the mandatory training requirements.

(b) Been convicted of a criminal offense that would require reporting.

(c) Refused to submit to a drug screening or has produced a positive result on a drug screening, where the positive result cannot be explained to the Administration Division Supervisor’s satisfaction.

(d) Resigned or been terminated in advance of:

1. Being convicted of an offense that would require reporting.
2. A pending drug screening.

(e) Resigned or been terminated under any other circumstances that require reporting.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Drug- and Alcohol-Free Workplace

1005.1 PURPOSE AND SCOPE

The purpose of this policy is to establish clear and uniform guidelines regarding drugs and alcohol in the workplace (41 USC § 8103).

1005.2 POLICY

It is the policy of the Madison County Sheriff's Office to provide a drug- and alcohol-free workplace for all members.

1005.3 GENERAL GUIDELINES

Alcohol and drug use in the workplace or on department time can endanger the health and safety of department members and the public.

Members who have consumed an amount of an alcoholic beverage or taken any medication, or combination thereof, that would tend to adversely affect their mental or physical abilities shall not report for duty. Affected members shall notify the Shift Supervisor or appropriate supervisor as soon as the member is aware that he/she will not be able to report to work. If the member is unable to make the notification, every effort should be made to have a representative contact the supervisor in a timely manner. If the member is adversely affected while on-duty, he/she shall be immediately removed and released from work (see the Work Restrictions section in this policy).

1005.3.1 USE OF MEDICATIONS

Members should not use any medications that will impair their ability to safely and completely perform their duties. Any member who is medically required or has a need to take any such medication shall report that need to his/her immediate supervisor prior to commencing any on-duty status.

1005.3.2 MEDICAL CANNABIS

Possession, use, or being under the influence of medical cannabis on-duty is prohibited and may lead to disciplinary action (Va. Code § 40.1-27.4).

1005.4 MEMBER RESPONSIBILITIES

Members shall report for work in an appropriate mental and physical condition. Members are prohibited from purchasing, manufacturing, distributing, dispensing, possessing or using controlled substances or alcohol on department premises or on department time (41 USC § 8103). The lawful possession or use of prescribed medications or over-the-counter remedies is excluded from this prohibition.

Members who are authorized to consume alcohol as part of a special assignment shall not do so to the extent of impairing on-duty performance.

Members shall notify a supervisor immediately if they observe behavior or other evidence that they believe demonstrates that a fellow on-duty member is impaired due to drug or alcohol use.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Members are required to notify their immediate supervisors of any criminal drug statute charge or conviction for a violation occurring in the workplace no later than five days after such charge is brought or conviction rendered (41 USC § 8103).

1005.5 EMPLOYEE ASSISTANCE PROGRAM

There may be available a voluntary employee assistance program to assist those who wish to seek help for alcohol and drug problems (41 USC § 8103). Insurance coverage that provides treatment for drug and alcohol abuse also may be available. Employees should contact the Human Resources Department, their insurance providers or the employee assistance program for additional information. It is the responsibility of each employee to seek assistance before alcohol or drug problems lead to performance problems.

1005.6 WORK RESTRICTIONS

If a member informs a supervisor that he/she has consumed any alcohol, drug or medication that could interfere with a safe and efficient job performance, the member may be required to obtain clearance from his/her physician before continuing to work.

If the supervisor reasonably believes, based on objective facts, that a member is impaired by the consumption of alcohol or other drugs, the supervisor shall prevent the member from continuing work and shall ensure that he/she is safely transported away from the Department.

1005.7 SCREENING TESTS

A supervisor shall require an employee to submit to a screening under any the following circumstances:

(a) The supervisor reasonably believes, based upon objective facts, that the employee is under the influence of alcohol or drugs that are impairing his/her ability to perform duties safely and efficiently.

(b) The employee discharges a firearm in the performance of his/her duties (excluding training or authorized euthanizing of an animal).

(c) The employee discharges a firearm issued by the Department while off-duty, resulting in injury, death or substantial property damage.

(d) The employee drives a motor vehicle in the performance of his/her duties and becomes involved in an incident that results in bodily injury, death or substantial damage to property.

1005.7.1 SUPERVISOR RESPONSIBILITIES

The supervisor shall prepare a written record documenting the specific facts that led to the decision to require the test, and shall inform the employee in writing of the following:

(a) The test will be given to detect either alcohol or drugs, or both.

(b) The result of the test is not admissible in any criminal proceeding against the employee.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) The employee may refuse the test, but refusal may result in dismissal or other disciplinary action.

1005.7.2 DISCIPLINE

An employee may be subject to disciplinary action if he/she:

(a) Fails or refuses to submit to a screening test.

(b) After taking a screening test that indicates the presence of a controlled substance, fails to provide proof, within 72 hours after being requested, that he/she took the controlled substance as directed, pursuant to a current and lawful prescription issued in his/her name.

1005.7.3 SAMPLE COLLECTION AND TESTING

Any blood or urine sample collected will be divided into two samples and the second sample will be preserved and made available should the employee wish to obtain subsequent independent analysis. An employee may request a subsequent test using the second sample by notifying the Sheriff in writing within 10 days of receiving notice of a positive test. In this event, the disciplinary action may be suspended until the confirmation test results are obtained (Va. Code § 9.1-501). The employee shall pay all costs of the confirmation test unless the confirmation test reverses the findings of the positive test.

Subsequent testing by the employee should follow the general standards as would apply to the testing standards used in a driving under the influence (DUI) investigation set forth in Va. Code § 18.2-268.1 through Va. Code § 18.2-268.12 (Va. Code § 9.1-501).

1005.8 COMPLIANCE WITH THE DRUG-FREE WORKPLACE ACT

No later than 30 days following notice of any drug statute conviction for a violation occurring in the workplace involving a member, the Department will take appropriate disciplinary action, up to and including dismissal, and/or requiring the member to satisfactorily participate in a drug abuse assistance or rehabilitation program (41 USC § 8104).

1005.9 CONFIDENTIALITY

The Department recognizes the confidentiality and privacy due to its members. Disclosure of any information relating to substance abuse treatment, except on a need-to-know basis, shall only be with the express written consent of the member involved or pursuant to lawful process.

The written results of any screening tests and all documents generated by the employee assistance program are considered confidential medical records and shall be maintained in the member’s confidential medical file in accordance with the Personnel Records Policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Sick Leave

1006.1 PURPOSE AND SCOPE

This policy provides general guidance regarding the use and processing of sick leave. The accrual and terms of use of sick leave for eligible employees are detailed in the applicable department manual.

This policy is not intended to cover all types of sick or other leaves. For example, employees may be entitled to additional paid or unpaid leave for certain family and medical reasons as provided for in the Family and Medical Leave Act (FMLA) (29 USC § 2601 et seq.).

1006.2 POLICY

It is the policy of the Madison County Sheriff's Office to provide eligible employees with a sick leave benefit.

1006.3 USE OF SICK LEAVE

Sick leave is intended to be used for qualified absences. Sick leave is not considered vacation. Abuse of sick leave may result in discipline, denial of sick leave benefits, or both.

Employees on sick leave shall not engage in other employment or self-employment or participate in any sport, hobby, recreational activity or other activity that may impede recovery from the injury or illness (see the Outside Employment and Outside Overtime Policy).

Qualified appointments should be scheduled during a member’s non-working hours when it is reasonable to do so.

1006.3.1 NOTIFICATION

All members should notify the Shift Supervisor or appropriate supervisor as soon as they are aware that they will not be able to report to work and no less than six hours before the start of their scheduled shifts. If, due to an emergency, a member is unable to contact the supervisor, every effort should be made to have a representative for the member contact the supervisor.

When the necessity to be absent from work is foreseeable, such as planned medical appointments or treatments, the member shall, whenever possible and practicable, provide the Department with no less than 30 days' notice of the impending absence.

Upon return to work, members are responsible for ensuring their time off was appropriately accounted for, and for completing and submitting the required documentation describing the type of time off used and the specific amount of time taken.

1006.4 EXTENDED ABSENCE

Members absent from duty for more than three consecutive days shall be required to furnish a statement from a health care provider supporting the need to be absent and/or the ability to return to work without limitation. Members on an extended absence shall, if possible, contact their supervisor at specified intervals to provide an update on their absence and expected date of return.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Nothing in this section precludes a supervisor from requiring, with cause, a health care provider's statement for an absence of three or fewer days.

1006.5 SUPERVISOR RESPONSIBILITIES

The responsibilities of supervisors include, but are not limited to:

(a) Monitoring and regularly reviewing the attendance of those under their command to ensure that the use of sick leave and absences is consistent with this policy.

(b) Attempting to determine whether an absence of four or more days may qualify as family medical leave and consulting with legal counsel or the Human Resources Department as appropriate.

(c) Addressing absences and sick leave use in the member’s performance evaluation when excessive or unusual use has:

1. Negatively affected the member’s performance or ability to complete assigned duties.
2. Negatively affected department operations.

(d) When appropriate, counseling members regarding excessive absences and/or inappropriate use of sick leave.

(e) Referring eligible members to an available employee assistance program when appropriate.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Communicable Diseases

1007.1 PURPOSE AND SCOPE

This policy provides general guidelines to assist in minimizing the risk of department members contracting and/or spreading communicable diseases.

1007.1.1 DEFINITIONS

Definitions related to this policy include:

Communicable disease - A human disease caused by microorganisms that are present in and transmissible through human blood, bodily fluid, tissue, or by breathing or coughing. These diseases commonly include, but are not limited to, hepatitis B virus (HBV), HIV and tuberculosis.

Exposure - When an eye, mouth, mucous membrane or non-intact skin comes into contact with blood or other potentially infectious materials, or when these substances are injected or infused under the skin; when an individual is exposed to a person who has a disease that can be passed through the air by talking, sneezing or coughing (i.e., tuberculosis), or the individual is in an area that was occupied by such a person. Exposure only includes those instances that occur due to a member’s position at the Madison County Sheriff's Office. (See the exposure control plan for further details to assist in identifying whether an exposure has occurred.)

1007.2 POLICY

The Madison County Sheriff's Office is committed to providing a safe work environment for its members. Members should be aware that they are ultimately responsible for their own health and safety.

1007.3 EXPOSURE CONTROL OFFICER

The Sheriff will assign a person as the Exposure Control Officer (ECO). The ECO shall develop an exposure control plan that includes:

(a) Exposure prevention and decontamination procedures (6 VAC 15-40-393).

(b) Procedures for when and how to obtain medical attention in the event of an exposure or suspected exposure.

(c) The provision that department members will have no-cost access to the appropriate personal protective equipment (PPE) (i.e., gloves, face masks, eye protection, pocket masks) that is appropriate for each member's position and risk of exposure.

(d) Evaluation of persons in custody for any exposure risk and measures to separate them.

(e) Compliance with all relevant laws or regulations related to communicable diseases, including:

1. Responding to requests and notifications regarding exposures covered under the Ryan White law (42 USC § 300ff-133; 42 USC § 300ff-136).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. Exposure control mandates for blood borne pathogens in 29 CFR 1910.1030 (Va. Code § 40.1-51.1; 16 VAC 25-90-1910).
3. Reporting any outbreak of a recordable disease, as identified by the State Board of Health, to the local health director or State Health Commissioner (Va. Code § 32.1-37).
4. Notifying emergency medical services personnel and/or an infection control officer of a receiving facility when a person who is in the custody of this department is known to have a communicable disease or is subject to a quarantine order prior to being transferred for medical treatment (Va. Code § 32.1-116.3).
5. Establishing procedures for the safe handling, storage and use of sharps by members (6 VAC 15-40-395).

The ECO should also act as the liaison with the Virginia Occupational Safety and Health (VOSH) Program and may request voluntary compliance inspections. The ECO should annually review and update the exposure control plan and review implementation of the plan.

1007.4 EXPOSURE PREVENTION AND MITIGATION

1007.4.1 GENERAL PRECAUTIONS

All members are expected to use good judgment and follow training and procedures related to mitigating the risks associated with communicable disease. This includes, but is not limited to (29 CFR 1910.1030; 16 VAC 25-90-1910):

(a) Stocking disposable gloves, antiseptic hand cleanser, CPR masks or other specialized equipment in the work area of department vehicles, as applicable.

(b) Wearing department-approved disposable gloves when contact with blood, other potentially infectious materials, mucous membranes and non-intact skin can be reasonably anticipated.

(c) Washing hands immediately or as soon as feasible after removal of gloves or other PPE.

(d) Treating all human blood and bodily fluids/tissue as if it is known to be infectious for a communicable disease.

(e) Using an appropriate barrier device when providing CPR.

(f) Using a face mask or shield if it is reasonable to anticipate an exposure to an airborne transmissible disease.

(g) Decontaminating non-disposable equipment (e.g., flashlight, control devices, clothing, portable radio) as soon as possible if the equipment is a potential source of exposure.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1. Clothing that has been contaminated by blood or other potentially infectious materials shall be removed immediately or as soon as feasible and stored/ decontaminated appropriately.

(h) Handling all sharps and items that cut or puncture (e.g., needles, broken glass, razors, knives) cautiously and using puncture-resistant containers for their storage and/or transportation.

(i) Avoiding eating, drinking, smoking, applying cosmetics or lip balm, or handling contact lenses where there is a reasonable likelihood of exposure.

(j) Disposing of biohazardous waste appropriately or labeling biohazardous material properly when it is stored.

1007.4.2 IMMUNIZATIONS
Members who could be exposed to HBV due to their positions may receive the HBV vaccine and any routine booster at no cost (29 CFR 1910.1030; 16 VAC 25-90-1910).

1007.5 POST EXPOSURE

1007.5.1 INITIAL POST-EXPOSURE STEPS
Members who experience an exposure or suspected exposure shall (29 CFR 1910.1030; 16 VAC 25-90-1910):

(a) Begin decontamination procedures immediately (e.g., wash hands and any other skin with soap and water, flush mucous membranes with water).

(b) Obtain medical attention as appropriate.

(c) Notify a supervisor as soon as practical.

1007.5.2 REPORTING REQUIREMENTS
The supervisor on-duty shall investigate every exposure or suspected exposure that occurs as soon as possible following the incident. The supervisor shall ensure the following information is documented (29 CFR 1910.1030; 16 VAC 25-90-1910):

(a) Name of the member exposed

(b) Date and time of incident

(c) Location of incident

(d) Potentially infectious materials involved and the source of exposure (e.g., identification of the person who may have been the source)

(e) Work being done during exposure

(f) How the incident occurred or was caused

(g) PPE in use at the time of the incident

(h) Actions taken post-event (e.g., clean-up, notifications)

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

The supervisor shall advise the member that disclosing the identity and/or infectious status of a source to the public or to anyone who is not involved in the follow-up process is prohibited. The supervisor should complete the incident documentation in conjunction with other reporting requirements that may apply (see the Work-Related Disease, Injury and Death Reporting and Illness and Injury Prevention policies).

1007.5.3 MEDICAL CONSULTATION, EVALUATION AND TREATMENT

Department members shall have the opportunity to have a confidential medical evaluation immediately after an exposure and follow-up evaluations as necessary.

The ECO should request a written opinion/evaluation from the treating medical professional that contains only the following information (29 CFR 1910.1030; 16 VAC 25-90-1910):

(a) Whether the member has been informed of the results of the evaluation.

(b) Whether the member has been notified of any medical conditions resulting from exposure to blood or other potentially infectious materials which require further evaluation or treatment.

No other information should be requested or accepted by the ECO.

1007.5.4 COUNSELING

The Department shall provide the member, and his/her family if necessary, the opportunity for counseling and consultation regarding the exposure (29 CFR 1910.1030; 16 VAC 25-90-1910).

1007.5.5 SOURCE TESTING

Testing a person for communicable diseases when that person was the source of an exposure should be done when it is desired by the exposed member or when it is otherwise appropriate. Source testing is the responsibility of the ECO. If the ECO is unavailable to seek timely testing of the source, it is the responsibility of the exposed member’s supervisor to ensure testing is sought.

Source testing may be achieved by:

(a) Obtaining consent from the individual.

(b) Seeking testing of the source if the member is exposed to bodily fluids that may transmit HIV or HBV or hepatitis C (Va. Code § 32.1-45.1; Va. Code § 32.1-45.2).

Since there is the potential for overlap between the different manners in which source testing may occur, the ECO is responsible for coordinating the testing to prevent unnecessary or duplicate testing.

The ECO should seek the consent of the individual for testing and consult the County Attorney to discuss other options when no statute exists for compelling the source of an exposure to undergo testing if he/she refuses.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1007.6 CONFIDENTIALITY OF REPORTS

Medical information shall remain in confidential files and shall not be disclosed to anyone without the member's written consent (except as required by law). Test results from persons who may have been the source of an exposure are to be kept confidential as well.

1007.7 TRAINING

All members shall participate in training regarding communicable diseases commensurate with the requirements of their position. The training (29 CFR 1910.1030; 16 VAC 25-90-1910):

(a) Shall be provided at the time of initial assignment to tasks where an occupational exposure may take place and at least annually after the initial training.

(b) Shall be provided whenever the member is assigned new tasks or procedures affecting his/her potential exposure to communicable disease.

(c) Should provide guidance on what constitutes an exposure, what steps can be taken to avoid an exposure and what steps should be taken if a suspected exposure occurs.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Smoking and Tobacco Use

1008.1 PURPOSE AND SCOPE

This policy establishes limitations on smoking and the use of tobacco products by members and others while on-duty or while in Madison County Sheriff's Office facilities or vehicles.

For the purpose of this policy, smoking and tobacco use includes, but is not limited to, any tobacco product, such as cigarettes, cigars, pipe tobacco, snuff, tobacco pouches and chewing tobacco, as well as any device that is intended to simulate smoking, such as an electronic cigarette or personal vaporizer.

1008.2 POLICY

The Madison County Sheriff's Office recognizes that tobacco use is a health risk and can be offensive to others. Smoking and tobacco use also presents an unprofessional image for the Department and its members. Therefore smoking and tobacco use is prohibited by members and visitors in all department facilities, buildings and vehicles, and as is further outlined in this policy.

1008.3 SMOKING AND TOBACCO USE

Smoking and tobacco use by members is prohibited any time members are in public view representing the Madison County Sheriff's Office.

It shall be the responsibility of each member to ensure that no person under his/her supervision smokes or uses any tobacco product inside County facilities and vehicles.

1008.4 ADDITIONAL PROHIBITIONS

The Madison County Sheriff's Office may regulate smoking inside County facilities and may designate reasonable no-smoking areas, considering the nature of the use and the size of the building (Va. Code § 15.2-2823).

The County of Madison County, Virginia may enact an ordinance that shall designate reasonable no smoking areas, considering the nature of the use and the size of the building (Va. Code § 15.2-2830). Members shall enforce violations of a no smoking ordinance as provided by law (Va. Code § 15.2-2833).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Personnel Complaints

1009.1 PURPOSE AND SCOPE

This policy provides guidelines for the reporting, investigation and disposition of complaints regarding the conduct of members of the Madison County Sheriff's Office. This policy shall not apply to any questioning, counseling, instruction, informal verbal admonishment or other routine or unplanned contact of a member in the normal course of duty, by a supervisor or any other member, nor shall this policy apply to a criminal investigation (Va. Code § 9.1-506).

1009.2 POLICY

The Madison County Sheriff's Office takes seriously all complaints regarding the service provided by the Department and the conduct of its members.

The Department will accept and address all complaints of misconduct in accordance with this policy and applicable federal, state and local law and municipal and county rules.

It is also the policy of this department to ensure that the community can report misconduct without concern for reprisal or retaliation.

Department administrative investigations process and procedure are available to all personnel.

1009.3 PERSONNEL COMPLAINTS

Personnel complaints include any allegation of misconduct or improper job performance that, if true, would constitute a violation of department policy or federal, state or local law, policy or rule. Personnel complaints may be generated internally or by the public.

Inquiries about conduct or performance that, if true, would not violate department policy or federal, state or local law, policy or rule may be handled informally by a supervisor and shall not be considered a personnel complaint. Such inquiries generally include clarification regarding policy, procedures or the response to specific incidents by the Department.

The Internal Affairs Unit is responsible for internal affairs and personnel complaints investigations.

1009.3.1 COMPLAINT CLASSIFICATIONS

Personnel complaints shall be classified in one of the following categories:

Informal - A matter in which the Shift Supervisor is satisfied that appropriate action has been taken by a supervisor of rank greater than the accused member.

Formal - A matter in which a supervisor determines that further action is warranted. Such complaints may be investigated by a supervisor of rank greater than the accused member or referred to the Internal Affairs Unit, depending on the seriousness and complexity of the investigation.

Incomplete - A matter in which the complaining party either refuses to cooperate or becomes unavailable after diligent follow-up investigation. At the discretion of the assigned supervisor or

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

the Internal Affairs Unit, such matters may be further investigated depending on the seriousness of the complaint and the availability of sufficient information.

1009.3.2 SOURCES OF COMPLAINTS

The following applies to the source of complaints:

(a) Individuals from the public may make complaints in any form, including in writing, by email, in person or by telephone.

1. Upon request and as practicable, assistance shall be provided to an individual filing a written complaint (Va. Code § 9.1-600).

(b) Any department member becoming aware of alleged misconduct shall immediately notify a supervisor.

(c) Supervisors shall initiate a complaint based upon observed misconduct or receipt from any source alleging misconduct that, if true, could result in disciplinary action.

(d) Anonymous and third-party complaints should be accepted and investigated to the extent that sufficient information is provided.

(e) Tort claims and lawsuits may generate a personnel complaint.

1009.4 AVAILABILITY AND ACCEPTANCE OF COMPLAINTS

1009.4.1 COMPLAINT FORMS

Personnel complaint forms will be maintained in a clearly visible location in the public area of the sheriff's facility and be accessible through the department website (Va. Code § 9.1-600).

Personnel complaint forms in languages other than English may also be provided, as determined necessary or practicable.

See attachment: Citizen Complaint (Rev. March 2022).pdf

1009.4.2 ACCEPTANCE

All complaints will be courteously accepted by any department member and promptly referred to the appropriate supervisor. Although written complaints are preferred, a complaint may also be filed orally, either in person or by telephone. Such complaints will be directed to a supervisor. If a supervisor is not immediately available to take an oral complaint, the receiving member shall obtain contact information sufficient for the supervisor to contact the complainant. The supervisor, upon contact with the complainant, shall complete and submit a complaint form as appropriate.

Although not required, complainants should be encouraged to file complaints in person so that proper identification, signatures, photographs or physical evidence may be obtained as necessary.

1009.5 DOCUMENTATION

The Department shall ensure that all formal and informal complaints are documented on a complaint form and that the nature of the complaint is defined as clearly as possible. The Department will process and conduct appropriate investigations of all complaints against the

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Department or its members, regardless of the source in order to maintain the integrity of the Department.

All complaints and inquiries shall be documented in a log that records and tracks complaints. The log shall include the nature of the complaint and the dispositions. On an annual basis, the Department should audit the log and send an audit report to the Sheriff or the authorized designee.

1009.6 INTERNAL AFFAIRS UNIT

The responsibilities of the Internal Affairs Unit include, but are not limited to:

(a) The coordination of all administrative investigations.

(b) The conducting of/or assigning administrative investigations.

(c) Serving as the repository for all active administrative investigation files.

(d) Assuring the timely completion of administrative investigations.

(e) Assuring compliance with the administrative investigation process.

(f) Classifying complaints.

(g) Maintaining the confidentiality of investigations assigned to the unit.

1009.6.1 INTERNAL AFFAIRS UNIT SUPERVISOR

The Internal Affairs Unit supervisor is selected by the Sheriff and reports to the Sheriff or his/her designee. The Internal Affairs Unit supervisor is responsible for supervising any member assigned to the Internal Affairs Unit, or any member assigned to an investigation originating from the Internal Affairs Unit. The Internal Affairs Unit supervisor shall oversee all of the responsibilities assigned to the Internal Affairs Unit and shall ensure that all directives related to the Internal Affairs Unit are disseminated to all members of the Madison County Sheriff's Office.

1009.7 ADMINISTRATIVE INVESTIGATIONS

The procedures relating to administrative investigations shall be disseminated to all members. Allegations of misconduct will be administratively investigated as follows.

1009.7.1 SUPERVISOR RESPONSIBILITIES

In general, the primary responsibility for the investigation of a personnel complaint shall rest with the member's immediate supervisor, unless the supervisor is the complainant, or the supervisor is the ultimate decision-maker regarding disciplinary action or has any personal involvement regarding the alleged misconduct. The Sheriff or the authorized designee may direct that another supervisor investigate any complaint.

A supervisor who becomes aware of alleged misconduct shall take reasonable steps to prevent aggravation of the situation.

The responsibilities of supervisors include, but are not limited to:

(a) Ensuring that upon receiving or initiating any formal complaint, a complaint form is completed.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1. The original complaint form will be directed to the Shift Supervisor of the accused member, via the chain of command, who will take appropriate action and/or determine who will have responsibility for the investigation.
2. In circumstances where the integrity of the investigation could be jeopardized by reducing the complaint to writing or where the confidentiality of a complainant is at issue, a supervisor shall orally report the matter to the member's Division Supervisor or the Sheriff, who will initiate appropriate action.

(b) Responding to all complaints in a courteous and professional manner.

(c) Resolving those personnel complaints that can be resolved immediately.

1. Follow-up contact with the complainant should be made within 24 hours of the Department receiving the complaint.
2. If the matter is resolved and no further action is required, the supervisor will note the resolution on a complaint form and forward the form to the Shift Supervisor.

(d) Ensuring that upon receipt of a complaint involving allegations of a potentially serious nature, the Shift Supervisor and Sheriff are notified via the chain of command as soon as practicable.

(e) Forwarding unresolved personnel complaints to the Shift Supervisor, who will determine whether to contact the complainant or assign the complaint for investigation.

(f) Informing the complainant of the investigator's name and the complaint number within three days after assignment.

(g) Investigating a complaint as follows:

1. Making reasonable efforts to obtain names, addresses and telephone numbers of witnesses.
2. When appropriate, ensuring immediate medical attention is provided and photographs of alleged injuries and accessible uninjured areas are taken.

(h) Ensuring that the procedural rights of the accused member are followed.

(i) Ensuring interviews of the complainant are generally conducted during reasonable hours.

In the case of a complaint that relates to sexual, racial, ethnic or other forms of prohibited harassment or discrimination, the Sheriff or assigned Internal Affairs Unit investigator shall promptly contact the Human Resources Department for direction.

1009.7.2 ADMINISTRATIVE INVESTIGATION PROCEDURES

Whether conducted by a supervisor or a member of the Internal Affairs Unit, the following applies to employees:

(a) Interviews of an accused employee shall be conducted during reasonable hours and preferably when the employee is on-duty. If the employee is off-duty, he/she shall be compensated.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Unless waived by the employee, interviews of an accused employee shall be at the Madison County Sheriff's Office or other reasonable and appropriate place.

(c) No more than two interviewers should ask questions of an accused employee.

(d) Prior to any interview, an employee shall be provided written notice of the nature of the investigation, the employee's rights relative to the investigation and the employee's responsibilities.

(e) All interviews should be for a reasonable period and the employee's personal needs should be accommodated.

(f) No employee should be subjected to offensive or threatening language, nor shall any promises, rewards or other inducements be used to obtain answers. Any employee refusing to answer questions directly related to the investigation may be ordered to answer questions administratively and may be subject to discipline for failing to do so.

(g) The interviewer should record all interviews of employees and witnesses. The employee may also record the interview. If the employee has been previously interviewed, a copy of that recorded interview shall be provided to the employee prior to any subsequent interview.

(h) All employees subjected to interviews that could result in discipline have the right to have an uninvolved representative present during the interview. However, in order to maintain the integrity of each individual’s statement, involved employees shall not consult or meet with a representative or attorney collectively or in groups prior to being interviewed.

(i) All employees shall provide complete and truthful responses to questions posed during interviews.

(j) No employee may be compelled to submit to a polygraph examination, nor shall any refusal to submit to such examination be mentioned in any investigation (Va. Code § 40.1-51.4:4).

1009.7.3 ADMINISTRATIVE INVESTIGATION FORMAT

Formal investigations of personnel complaints shall be thorough, complete and essentially follow this format:

Introduction - Include the identity of the members, the identity of the assigned investigators, the initial date and source of the complaint.

Synopsis - Provide a brief summary of the facts giving rise to the investigation.

Summary - List the allegations separately, including applicable policy sections, with a brief summary of the evidence relevant to each allegation. A separate recommended finding should be provided for each allegation.

Evidence - Each allegation should be set forth with the details of the evidence applicable to each allegation provided, including comprehensive summaries of member and witness statements. Other evidence related to each allegation should also be detailed in this section.

Conclusion - A recommendation regarding further action or disposition should be provided.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Exhibits - A separate list of exhibits (e.g., recordings, photos, documents) should be attached to the report.

1009.7.4 DISPOSITIONS
Each personnel complaint shall be classified with one of the following dispositions:

Unfounded - When the investigation discloses that the alleged acts did not occur or did not involve department members. Complaints that are determined to be frivolous will fall within the classification of unfounded.

Exonerated - When the investigation discloses that the alleged act occurred but that the act was justified, lawful and/or proper.

Not sustained - When the investigation discloses that there is insufficient evidence to sustain the complaint or fully exonerate the member.

Sustained - When the investigation discloses sufficient evidence to establish that the act occurred and that it constituted misconduct.

If an investigation discloses misconduct or improper job performance that was not alleged in the original complaint, the investigator shall take appropriate action with regard to any additional allegations.

1009.7.5 COMPLETION OF INVESTIGATIONS
Every investigator or supervisor assigned to investigate a personnel complaint or other alleged misconduct shall proceed with due diligence in an effort to complete the investigation within one year from the date of discovery by an individual authorized to initiate an investigation.

1009.7.6 NOTICE TO COMPLAINANT OF INVESTIGATION STATUS
The member conducting the investigation should provide the complainant with periodic updates on the status of the investigation, as appropriate.

1009.7.7 NOTICE TO EMPLOYEE OF INVESTIGATION STATUS
The member conducting the investigation should provide the employee who is the subject of the investigation with periodic updates on the status of the investigation, as appropriate.

1009.8 ADMINISTRATIVE SEARCHES
Assigned lockers, storage spaces and other areas, including desks, offices and vehicles, may be searched as part of an administrative investigation upon a reasonable suspicion of misconduct.

Such areas may also be searched any time by a supervisor for non-investigative purposes, such as obtaining a needed report, radio or other document or equipment.

1009.9 ADMINISTRATIVE LEAVE
When a complaint of misconduct is of a serious nature, or when circumstances indicate that allowing the accused to continue to work would adversely affect the mission of the Department, the

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Sheriff or the authorized designee may temporarily assign an accused employee to administrative leave. Any employee placed on administrative leave:

(a) May be required to relinquish any department badge, identification, assigned weapons and any other department equipment.

(b) Shall be required to continue to comply with all policies and lawful orders of a supervisor.

(c) May be temporarily reassigned to a different shift, generally a normal business-hours shift, during the investigation. The employee may be required to remain available for contact at all times during such shift and will report as ordered.

1009.10 CRIMINAL INVESTIGATION

Where a member is accused of potential criminal conduct, a separate supervisor or investigator shall be assigned to investigate the criminal allegations apart from any administrative investigation. Any separate administrative investigation may parallel a criminal investigation.

The Sheriff shall be notified as soon as practicable when a member is accused of criminal conduct. The Sheriff may request a criminal investigation by an outside law enforcement agency.

A member accused of criminal conduct shall be provided with all rights afforded to a civilian. The member should not be administratively ordered to provide any information in the criminal investigation.

The Madison County Sheriff's Office may release information concerning the arrest or detention of any member, including a deputy, that has not led to a conviction. No disciplinary action should be taken until an independent administrative investigation is conducted.

1009.11 POST-ADMINISTRATIVE INVESTIGATION PROCEDURES

Upon completion of a formal investigation, an investigation report should be forwarded to the Sheriff through the chain of command. Each level of command should review the report and include their comments in writing before forwarding the report. The Sheriff may accept or modify any classification or recommendation for disciplinary action.

1009.11.1 DIVISION SUPERVISOR RESPONSIBILITIES

Upon receipt of any completed personnel investigation, the Division Supervisor of the involved member shall review the entire investigative file, the member's personnel file and any other relevant materials.

The Division Supervisor may make recommendations regarding the disposition of any allegations and the amount of discipline, if any, to be imposed.

Prior to forwarding recommendations to the Sheriff, the Division Supervisor may return the entire investigation to the assigned investigator or supervisor for further investigation or action.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

When forwarding any written recommendation to the Sheriff, the Division Supervisor shall include all relevant materials supporting the recommendation. Actual copies of a member's existing personnel file need not be provided and may be incorporated by reference.

1009.11.2 SHERIFF RESPONSIBILITIES

Upon receipt of any written recommendation for disciplinary action, the Sheriff shall review the recommendation and all accompanying materials. The Sheriff may modify any recommendation and/or may return the file to the Division Supervisor for further investigation or action.

Once the Sheriff is satisfied that no further investigation or action is required by staff, the Sheriff shall determine the amount of discipline, if any, that should be imposed, and whether remedial training, counseling or other punitive actions are warranted. In the event disciplinary action is proposed, the Sheriff shall provide the member with a written notice and the following:

(a) Access to all of the materials considered by the Sheriff in recommending the proposed discipline.

(b) An opportunity to respond orally and in writing to the Sheriff within five days of receiving the notice.

1. Upon a showing of good cause by the member, the Sheriff may grant a reasonable extension of time for the member to respond.

2. If the member elects to respond orally, the presentation shall be recorded by the Department. Upon request, the member shall be provided with a copy of the recording.

Once the member has completed his/her response, or if the member has elected to waive any such response, the Sheriff shall consider all information received in regard to the recommended discipline. The Sheriff shall render a timely written decision to the member and specify the grounds and reasons for discipline and the effective date of the discipline. Once the Sheriff has issued a written decision, the discipline shall become effective.

1009.11.3 NOTICE OF FINAL DISPOSITION TO THE COMPLAINANT

The Sheriff or the authorized designee should ensure that the complainant is notified of the disposition (i.e., sustained, not sustained, exonerated, unfounded) of the complaint.

1009.12 PRE-DISCIPLINE EMPLOYEE RESPONSE

The pre-discipline process is intended to provide the accused employee with an opportunity to present a written or oral response to the Sheriff after having had an opportunity to review the supporting materials and prior to imposition of any recommended discipline. The employee shall consider the following:

(a) The response is not intended to be an adversarial or formal hearing.

(b) Although the employee may be represented by an uninvolved representative or legal counsel, the response is not designed to accommodate the presentation of testimony or witnesses.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(c) The employee may suggest that further investigation could be conducted or the employee may offer any additional information or mitigating factors for the Sheriff to consider.

(d) In the event that the Sheriff elects to conduct further investigation, the employee shall be provided with the results prior to the imposition of any discipline.

(e) The employee may thereafter have the opportunity to further respond orally or in writing to the Sheriff on the limited issues of information raised in any subsequent materials.

1009.13 RESIGNATIONS/RETIREMENTS PRIOR TO DISCIPLINE

In the event that a member tenders a written resignation or notice of retirement prior to the imposition of discipline, it shall be noted in the file. The tender of a resignation or retirement by itself shall not serve as grounds for the termination of any pending investigation or discipline.

1009.14 RETENTION OF PERSONNEL INVESTIGATION FILES

All personnel complaints shall be maintained in accordance with the established records retention schedule and as described in the Personnel Records Policy (Va. Code § 9.1-600).

All complaint records and internal affairs investigations shall be considered confidential and secured appropriately. Internal investigation files are the property of the Department and access is restricted to those overseeing the investigation, imposing discipline or administratively processing.

1009.15 PROBATIONARY EMPLOYEES AND OTHER MEMBERS

At-will and probationary employees and members other than non-probationary employees may be disciplined and/or released from employment without adherence to any of the procedures set out in this policy, and without notice or cause at any time. These individuals are not entitled to any rights under this policy. However, any of these individuals released for misconduct should be afforded an opportunity solely to clear their names through a liberty interest hearing, which shall be limited to a single appearance before the Sheriff or the authorized designee.

In cases where an individual has been absent for more than a week or when additional time to review the individual is considered to be appropriate, the probationary period may be extended at the discretion of the Sheriff.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Safety Belts

1010.1 PURPOSE AND SCOPE

This policy establishes guidelines for the use of safety belts and child restraints. This policy will apply to all members operating or riding in department vehicles.

1010.1.1 DEFINITIONS

Definitions related to this policy include:

Child restraint system - An infant or child passenger restraint system that meets Federal Motor Vehicle Safety Standards and regulations set forth in 49 CFR 571.213 and Va. Code § 46.2-1095.

1010.2 POLICY

It is the policy of the Madison County Sheriff's Office that members use safety and child restraint systems to reduce the possibility of death or injury in a motor vehicle accident.

1010.3 WEARING OF SAFETY RESTRAINTS

All members shall wear properly adjusted safety restraints when operating or riding in a seat equipped with restraints, in any vehicle owned, leased or rented by this department while on- or off-duty, or in any privately owned vehicle while on-duty. The member driving such a vehicle shall ensure that all other occupants, including those who are not members of the Department, are properly restrained.

Exceptions to the requirement to wear safety restraints may be made only in exceptional situations where, due to unusual circumstances, wearing a safety belt would endanger the department member or the public. Members must be prepared to justify any deviation from this requirement.

1010.4 TRANSPORTING CHILDREN

Child passengers shall be transported using an approved child restraint system in compliance with Va. Code § 46.2-1095, Va. Code § 46.2-1096 and Va. Code § 46.2-1100.

Rear seat passengers in a cage-equipped vehicle may have reduced clearance, which requires careful seating and positioning of safety belts. Due to this reduced clearance, and if permitted by law, children and any child restraint system may be secured in the front seat of such vehicles provided this positioning meets federal safety standards and the vehicle and child restraint system manufacturer’s design and use recommendations. In the event that a child is transported in the front seat of a vehicle, the seat should be pushed back as far as possible and the passenger-side airbag should be deactivated. If this is not possible, members should arrange alternate transportation when feasible.

1010.5 TRANSPORTING SUSPECTS, PRISONERS OR ARRESTEES

Suspects, prisoners and arrestees should be in a seated position and secured in the rear seat of any department vehicle with a prisoner restraint system or, when a prisoner restraint system is not available, by safety belts provided by the vehicle manufacturer. The prisoner restraint system is not intended to be a substitute for handcuffs or other appendage restraints.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Safety Belts

Prisoners in leg restraints shall be transported in accordance with the Handcuffing and Restraints Policy.

1010.6 INOPERABLE SAFETY BELTS

Department vehicles shall not be operated when the safety belt in the driver's position is inoperable. Persons shall not be transported in a seat in which the safety belt is inoperable.

Department vehicle safety belts shall not be modified, removed, deactivated or altered in any way, except by the vehicle maintenance and repair staff, who shall do so only with the express authorization of the Sheriff.

Members who discover an inoperable restraint system shall report the defect to the appropriate supervisor. Prompt action will be taken to replace or repair the system.

1010.7 VEHICLES MANUFACTURED WITHOUT SAFETY BELTS

Vehicles manufactured and certified for use without safety belts or other restraint systems are subject to the manufacturer’s operator requirements for safe use.

1010.8 VEHICLE AIRBAGS

In all vehicles equipped with airbag restraint systems, the system will not be tampered with or deactivated, except when transporting children as written elsewhere in this policy. All equipment installed in vehicles equipped with airbags will be installed as per the vehicle manufacturer specifications to avoid the danger of interfering with the effective deployment of the airbag device.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Body Armor

1011.1 PURPOSE AND SCOPE

The purpose of this policy is to provide deputies with guidelines for the proper use of body armor.

1011.2 POLICY

It is the policy of the Madison County Sheriff's Office to maximize deputy safety through the use of body armor in combination with prescribed safety procedures. While body armor provides a significant level of protection, it is not a substitute for the observance of deputy safety procedures.

1011.3 ISSUANCE

The Administration Division Supervisor shall ensure that body armor is issued to all deputies and that, when issued, the body armor meets or exceeds the standards of the National Institute of Justice.

Body armor shall be issued when a deputy begins service at the Madison County Sheriff's Office and shall be replaced when the body armor becomes worn or damaged to the point that its effectiveness or functionality has been compromised.

The Sheriff may authorize issuance of body armor to uniformed, non-sworn members whose jobs may make wearing of body armor advisable.

1011.3.1 USE

Generally, the required use of body armor is subject to the following:

(a) Members shall only wear department-approved body armor.

(b) Members shall wear body armor any time they are in a situation where they could reasonably be expected to take enforcement action.

(c) Members shall wear body armor when working in uniform. The wearing of body armor during firearms qualification is optional.

(d) Members are not required to wear body armor when they are functioning primarily in an administrative or support capacity and would not reasonably be expected to take enforcement action.

(e) Deputies may be excused from wearing body armor when they are involved in undercover or plainclothes work that their supervisor determines could be compromised by wearing body armor, or when a supervisor determines that other circumstances make it inappropriate to mandate wearing body armor.

1. In those instances when body armor is not worn, deputies should have reasonable access to their body armor.

1011.3.2 INSPECTION

Supervisors should ensure through routine observation and periodic documented inspections that body armor is worn and maintained in accordance with this policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Annual inspections of body armor should be conducted by a person trained to perform the inspection for fit, cleanliness and signs of damage, abuse and wear.

1011.3.3 CARE AND MAINTENANCE

The required care and maintenance of body armor is subject to the following:

(a) Members are responsible for inspecting their body armor for signs of damage, wear and cleanliness at the start of each shift.

1. Unserviceable body armor shall be reported to the supervisor.

(b) Members are responsible for the proper storage of their body armor.

1. Body armor should not be stored for an extended period of time in an area where environmental conditions (e.g., temperature, light, humidity) could potentially degrade its effectiveness.

(c) Members are responsible for the care and cleaning of their body armor pursuant to the manufacturer's care instructions.

1. Body armor should not be exposed to any cleaning agents or methods not specifically recommended by the manufacturer.

2. Failure to follow manufacturer's care instructions may damage the ballistic performance capabilities of the body armor. If care instructions for the body armor cannot be located, the manufacturer should be contacted to request the instructions.

(d) Body armor should be replaced in accordance with the manufacturer's recommended replacement schedule, or when its effectiveness or functionality has been compromised.

1011.4 RANGEMASTER RESPONSIBILITIES

The responsibilities of the Rangemaster include, but are not limited to:

(a) Monitoring technological advances in the body armor industry for any appropriate changes to department-approved body armor.

(b) Assessing the level of weapons and ammunition currently utilized by the public and the suitability of approved body armor to protect against those threats.

(c) Educating deputies about the safety benefits of wearing body armor.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Personnel Records

1012.1 PURPOSE AND SCOPE

This policy governs maintenance and access to personnel records. Personnel records include any file maintained under an individual member's name.

1012.2 POLICY

It is the policy of this department to maintain personnel records and preserve the confidentiality of personnel records pursuant to the Constitution and the laws of Virginia (Va. Code § 2.2-3705.1(1)).

1012.3 DEPARTMENT FILE

The department file shall be maintained as a record of a person’s employment/appointment with this department. The department file should contain, at a minimum:

(a) Personal data, including photographs, marital status, names of family members, educational and employment history or similar information. A photograph of the member should be permanently retained.

(b) Election of employee benefits.

(c) Personnel action reports reflecting assignments, promotions and other changes in employment/appointment status. These should be permanently retained.

(d) Original performance evaluations. These should be permanently maintained.

(e) Discipline records, including copies of sustained personnel complaints.

(f) Adverse comments such as supervisor notes or memos may be retained in the department file after the member has had the opportunity to read and initial the comment.

1. Once a member has had an opportunity to read and initial any adverse comment, the member shall be given the opportunity to respond in writing to the adverse comment.
2. Any member response shall be attached to and retained with the original adverse comment.
3. If a member refuses to initial or sign an adverse comment, at least one supervisor should note the date and time of such refusal on the original comment. Such a refusal, however, shall not be deemed insubordination, nor shall it prohibit the entry of the adverse comment into the member's file.

(g) Commendations and awards.

(h) Any other information, the disclosure of which would constitute an unwarranted invasion of personal privacy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1012.4 DIVISION FILE

Division files may be separately maintained internally by a member's supervisor for the purpose of completing timely performance evaluations. The Division file may contain supervisor comments, notes, notices to correct and other materials that are intended to serve as a foundation for the completion of timely performance evaluations.

1012.5 TRAINING FILE

An individual training file shall be maintained by the Training Supervisor for each member. Training files will contain records of all training; original or photocopies of available certificates, transcripts, diplomas and other documentation; and education and firearms qualifications. Training records may also be created and stored remotely, either manually or automatically (e.g., Daily Training Bulletin (DTB) records).

(a) The involved member is responsible for providing the Training Supervisor or immediate supervisor with evidence of completed training/education in a timely manner.

(b) The Training Supervisor or supervisor shall ensure that copies of such training records are placed in the member’s training file.

1012.6 INTERNAL AFFAIRS FILE

Internal affairs files shall be maintained under the exclusive control of the Internal Affairs Unit in conjunction with the office of the Sheriff. Access to these files may only be approved by the Sheriff or the Internal Affairs Unit supervisor.

These files shall contain the complete investigation of all formal complaints of member misconduct, regardless of disposition. Investigations of complaints that result in the following findings shall not be placed in the member's department file but will be maintained in the internal affairs file:

(a) Not sustained

(b) Unfounded

(c) Exonerated

1012.7 MEDICAL FILE

A medical file shall be maintained separately from all other personnel records and shall contain all documents relating to the member’s medical condition and history including, but not limited to:

(a) Materials relating to a medical leave of absence, including leave under the Family and Medical Leave Act (FMLA).

(b) Documents relating to workers’ compensation claims or the receipt of short- or long-term disability benefits.

(c) Fitness-for-duty examinations, psychological and physical examinations, follow-up inquiries and related documents.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Medical release forms, doctor’s slips and attendance records that reveal a member’s medical condition.

(e) Any other documents or materials that reveal the member’s medical history or medical condition, including past, present or future anticipated mental, psychological or physical limitations.

1012.8 SECURITY

Personnel records should be maintained in a secured location and locked either in a cabinet or access-controlled room. Personnel records maintained in an electronic format should have adequate password protection.

Personnel records are subject to disclosure only as provided in this policy, the Records Maintenance and Release Policy or according to applicable discovery procedures (Va. Code § 2.2-3705.1; Va. Code § 2.2-3706).

Nothing in this policy is intended to preclude review of personnel records by the County Administrator, County Attorney or other attorneys or representatives of the County in connection with official business.

1012.8.1 REQUESTS FOR DISCLOSURE

Any member receiving a request for a personnel record shall promptly notify the Custodian of Records or other person charged with the maintenance of such records.

Upon receipt of any such request, the responsible person shall notify the affected member as soon as practicable that such a request has been made.

The responsible person shall further ensure that an appropriate response to the request is made in a timely manner, consistent with applicable law. In many cases, this may require assistance of available legal counsel.

All requests for disclosure that result in access to a member’s personnel records shall be logged in the corresponding file.

1012.8.2 RELEASE OF PERSONNEL INFORMATION

The Department may release any factual information concerning a disciplinary investigation if the member who is the subject of the investigation (or the member's representative) publicly makes a statement that is published in the media and that the member (or representative) knows to be false. The disclosure of such information, if any, shall be limited to facts that refute any such false statement.

The Department should respond to a request from another law enforcement agency or jail for information related to a former deputy’s prior arrests, prosecutions, criminal conduct, excessive use of force, official misconduct, civil suits, or adverse employment actions, and provide the information required and permitted by law within 14 days (Va. Code § 15.2-1705).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1012.9 MEMBER ACCESS TO HIS/HER OWN PERSONNEL RECORDS

Any member or former employee may request access to his/her own personnel records during the normal business hours of those responsible for maintaining such files (Va. Code § 2.2-3705.1(1); Va. Code § 8.01-413.1).

Any member seeking the removal of any item from his/her personnel records shall file a written request to the Sheriff through the chain of command. The Department shall remove any such item if appropriate, or within 30 days provide the member with a written explanation of why the contested item will not be removed. If the contested item is not removed from the file, the member's request and the written response from the Department shall be retained with the contested item in the member's corresponding personnel record.

Members may be restricted from accessing files containing any of the following information:

(a) An ongoing internal affairs investigation to the extent that it could jeopardize or compromise the investigation pending final disposition or notice to the member of the intent to discipline.

(b) Confidential portions of internal affairs files that have not been sustained against the member.

(c) Criminal investigations involving the member.

(d) Letters of reference concerning employment/appointment, licensing, or issuance of permits regarding the member.

(e) Any portion of a test document, except the cumulative total test score for either a section of the test document or for the entire test document.

(f) Materials used by the Department for staff management planning, including judgments or recommendations concerning future salary increases and other wage treatments, management bonus plans, promotions and job assignments, or other comments or ratings used for Department planning purposes.

(g) Information of a personal nature about a person other than the member if disclosure of the information would constitute a clearly unwarranted invasion of the other person's privacy.

(h) Records relevant to any other pending claim between the Department and the member that may be discovered in a judicial proceeding.

1012.10 RETENTION AND PURGING

Unless provided otherwise in this policy, personnel records shall be maintained in accordance with the established records retention schedule.

(a) During the preparation of each member's performance evaluation, all personnel complaints and disciplinary actions should be reviewed to determine the relevancy, if any, to progressive discipline, training and career development. Each supervisor responsible for completing the member's performance evaluation should determine whether any prior sustained disciplinary file should be retained beyond the required period for reasons other than pending litigation or other ongoing legal proceedings.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) If a supervisor determines that records of prior discipline should be retained beyond the required period, approval for such retention should be obtained through the chain of command from the Sheriff.

(c) If, in the opinion of the Sheriff, a personnel complaint or disciplinary action maintained beyond the required retention period is no longer relevant, all records of such matter may be destroyed in accordance with the established records retention schedule.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Request for Change of Assignment

1013.1 PURPOSE AND SCOPE

This policy establishes guidelines for department members to request a change of assignment in response to an announced vacancy.

1013.2 POLICY

It is the policy of the Madison County Sheriff's Office that all requests for change of assignment be considered in an equitable and nondiscriminatory manner.

1013.3 REQUEST FOR CHANGE OF ASSIGNMENT

Members requesting a change of assignment shall submit a request document through the chain of command to their Division Supervisors. In the case of patrol deputies, the chain of command must include the Shift Supervisor.

The change of assignment request document provides members with the opportunity to list their qualifications for specific assignments. It should include:

(a) The member's relevant experience, education and training.

(b) All assignments in which the member is interested.

(c) Total years of service

The document will remain in effect until the end of the calendar year in which it was submitted. Effective January 1 of each year, members still interested in a change of assignment should complete and submit a new request.

1013.4 RESPONSIBILITIES

1013.4.1 SUPERVISORS

Upon receipt of a change of assignment request document, the supervisor shall make appropriate comments in the space provided on the document and forward it to the member's Division Supervisor.

In the case of patrol deputies, the Shift Supervisor shall make appropriate comments on the form regarding his/her recommendation and forward the request to the Division Supervisor.

1013.4.2 DIVISION SUPERVISORS

If the Division Supervisor receives a change of assignment request document from a patrol deputy that does not contain Shift Supervisor comments, he/she will make appropriate comments and return it to the member without consideration.

The Division Supervisor will review all change of assignment requests and submit his/her recommendation to the Sheriff.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Commendations and Awards

1014.1 PURPOSE AND SCOPE

This policy provides general guidelines for recognizing commendable or meritorious acts of members of the Madison County Sheriff's Office and individuals from the community.

1014.2 POLICY

It is the policy of the Madison County Sheriff's Office to recognize and acknowledge exceptional individual or group achievements, performance, proficiency, heroism and service of its members and individuals from the community through commendations and awards.

1014.3 COMMENDATIONS

Commendations for members of the Department or for individuals from the community may be initiated by any department member or by any person from the community.

1014.4 CRITERIA

A meritorious or commendable act may include, but is not limited to:

- Superior handling of a difficult situation.
- Conspicuous bravery or outstanding performance.
- Any action or performance that is above and beyond typical duties.

1014.4.1 DEPARTMENT MEMBER DOCUMENTATION

Members of the Department should document meritorious or commendable acts. The documentation should contain:

(a) Identifying information:

1. For members of the Department - name, division and assignment at the date and time of the meritorious or commendable act
2. For individuals from the community - name, address, telephone number

(b) A brief account of the meritorious or commendable act with report numbers, as appropriate.

(c) The signature of the member submitting the documentation.

1014.4.2 COMMUNITY MEMBER DOCUMENTATION

Documentation of a meritorious or commendable act submitted by a person from the community should be accepted in any form. However, written documentation is preferred. Department members accepting the documentation should attempt to obtain detailed information regarding the matter, including:

(a) Identifying information:

1. For members of the Department - name, division and assignment at the date and time of the meritorious or commendable act

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. For individuals from the community - name, address, telephone number

(b) A brief account of the meritorious or commendable act with report numbers, as appropriate.

(c) The signature of the person submitting the documentation.

1014.4.3 PROCESSING DOCUMENTATION

Documentation regarding the meritorious or commendable act of a member of the Department should be forwarded to the appropriate Division Supervisor for his/her review. The Division Supervisor should sign and forward the documentation to the Sheriff for his/her review.

The Sheriff or the authorized designee will present the commendation to the department member for his/her signature. The documentation will then be returned to the Administration secretary for entry into the member's personnel file.

Documentation regarding the meritorious or commendable act of an individual from the community should be forwarded to the Administration Division Supervisor. The documentation will be signed by the Division Supervisor and forwarded to the Sheriff for his/her review. An appropriate venue or ceremony to acknowledge the individual's actions should be arranged. Documentation of the commendation shall be maintained in a file designated for such records.

1014.5 AWARDS

Awards may be bestowed upon members of the Department and individuals from the community. These awards include:

- Award of Valor.
- Award of Merit.
- Lifesaving Award.
- Meritorious Conduct.

Criteria for each award and the selection, presentation and display of any award are determined by the Sheriff.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Fitness for Duty

1015.1 PURPOSE AND SCOPE

Monitoring members' fitness for duty is essential for the safety and welfare of the members of the Department and the community. The purpose of this policy is to ensure that all members of this department remain fit for duty and able to perform their job functions.

1015.2 POLICY

The Madison County Sheriff's Office strives to provide a safe and productive work environment and ensure that all members of this department can safely and effectively perform the essential functions of their jobs. Under limited circumstances, the Department may require at no cost to the employee a professional evaluation of a member's physical and/or mental capabilities to determine his/her ability to perform essential functions.

1015.3 MEMBER RESPONSIBILITIES

It is the responsibility of each member of this department to maintain physical stamina and psychological stability sufficient to safely and effectively perform the essential duties of his/her position. The Department will make available guidelines appropriate for each position.

During working hours, all members are required to be alert, attentive and capable of performing their assigned responsibilities.

Any member who feels unable to perform his/her duties shall promptly notify a supervisor. In the event that a member believes that another department member is unable to perform his/her duties, such observations and/or belief shall be promptly reported to a supervisor.

1015.4 SUPERVISOR RESPONSIBILITIES

All supervisors should be alert to any indication that a member may be unable to safely perform his/her duties due to an underlying physical or psychological impairment or condition.

Such indications may include:

(a) An abrupt and negative change in the member's normal behavior.

(b) A pattern of irrational conduct, hostility or oppositional behavior.

(c) Personal expressions of instability.

(d) Inappropriate use of alcohol or other substances, including prescribed medication.

(e) A pattern of questionable judgment, impulsive behavior or the inability to manage emotions.

(f) Any other factor or combination of factors causing a supervisor to believe the member may be suffering from an impairment or condition requiring intervention.

Supervisors shall maintain the confidentiality of any information consistent with this policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1015.4.1 REPORTING

A supervisor observing a member, or receiving a report of a member, who is perceived to be unable to safely or effectively perform his/her duties shall promptly document all objective information and/or observations.

The supervisor should attempt to meet with the member to inquire about the conduct or behavior giving rise to the concerns.

If a meeting does not resolve the supervisor's concerns or does not take place, the supervisor shall promptly document his/her observations and actions in a written report and inform the Shift Supervisor or the member's Division Supervisor.

1015.4.2 DUTY STATUS

In conjunction with the Shift Supervisor or the member's Division Supervisor, the supervisor should make a preliminary determination regarding the member's duty status.

If a determination is made that the member can safely and effectively perform the essential functions of his/her job, the member should be returned to duty and arrangements made for appropriate follow-up.

If a preliminary determination is made that the member's conduct or behavior represents an inability to safely and effectively perform the essential functions of his/her job, the Shift Supervisor or the member's Division Supervisor should immediately relieve the member of duty pending further evaluation.

Employees relieved of duty shall comply with the administrative leave provisions of the Personnel Complaints Policy.

The Sheriff shall be promptly notified in the event that any member is relieved of duty.

1015.5 FITNESS-FOR-DUTY EVALUATIONS

A fitness-for-duty evaluation may be ordered whenever circumstances reasonably indicate that a member is unfit for duty or following an officer-involved shooting or death-in-custody incident.

1015.5.1 PROCESS

The Sheriff may order the member to undergo a fitness-for-duty evaluation at no cost to the employee.

The examining practitioner will provide the Department with a report indicating whether the member is fit for duty. If the member is not fit for duty, the practitioner will include the existing restrictions or conditions in the report.

In order to facilitate the evaluation of any member, the Department will provide all appropriate documents and available information.

All reports and evaluations submitted by the examining practitioner shall be part of the member's confidential medical file.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Any member ordered to undergo a fitness-for-duty evaluation shall comply with the terms of the order and cooperate fully with the examining practitioner. Any failure to comply with such an order and any failure to cooperate with the practitioner may be deemed insubordination and shall subject the member to discipline, up to and including termination.

Determinations regarding duty status of members who are found to be unfit for duty or fit for duty with limitations will be made by the Sheriff.

1015.6 LIMITATION ON HOURS WORKED

Absent emergency operations, members should not work more than:

- 16 hours in a one-day (24 hours) period
- 30 hours in any two-day (48 hours) period
- 84 hours in any seven-day (168 hours) period

Except in unusual circumstances, members should have a minimum of eight hours off between shifts. Supervisors should give consideration to reasonable rest periods and are authorized to deny overtime or relieve any member who has exceeded the above guidelines to off-duty status.

Limitations on the number of hours worked apply to shift changes, shift trades, rotation, holdover, training, general overtime and any other work assignments.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Meal Periods and Breaks

1016.1 PURPOSE AND SCOPE

This policy provides general guidance regarding the availability of meal periods and breaks.

1016.2 POLICY

It is the policy of the Madison County Sheriff's Office to provide meal periods and breaks to members of this department.

1016.3 MEAL PERIODS

Deputies and dispatchers shall remain on-duty subject to call during meal periods. All other members are not on-call during meal periods unless directed otherwise by a supervisor.

Uniformed deputies shall take their meal periods within the County limits and shall monitor the sheriff's radio, unless on assignment outside of the County.

The time spent for the meal period shall not exceed the authorized time allowed.

1016.4 BREAKS

Each member is entitled to a 15-minute break for each four-hour work period. Only one break shall be taken during each four hours of duty. No breaks shall be taken during the first or last hour of a member's shift unless approved by a supervisor.

Members normally assigned to the sheriff's facility shall remain at the sheriff's facility for their breaks. This does not prohibit them from taking a break away from the facility if they are on official business or otherwise approved by a supervisor.

Members assigned to field duties will take their breaks in their assigned areas, subject to call, and shall monitor the sheriff's radio. When such members take their breaks away from their vehicles, they shall do so only with the knowledge and clearance of the dispatcher.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Lactation Breaks

1017.1 PURPOSE AND SCOPE

The purpose of this policy is to provide reasonable accommodations to members desiring to express breast milk for the member’s infant child.

1017.2 POLICY

It is the policy of the Madison County Sheriff's Office to provide, in compliance with the Fair Labor Standards Act (FLSA), reasonable break time and appropriate facilities to accommodate any member desiring to express breast milk for her infant nursing child for up to one year after the child’s birth (29 USC § 207).

1017.3 LACTATION BREAK TIME

A rest period should be permitted each time the member has the need to express breast milk (29 USC § 207; Va. Code § 2.2-3904). In general, lactation breaks that cumulatively total 30 minutes or less during any four-hour work period or major portion of a four-hour work period would be considered reasonable. However, individual circumstances may require more or less time.

Lactation breaks, if feasible, should be taken at the same time as the member’s regularly scheduled rest or meal periods. While a reasonable effort will be made to provide additional time beyond authorized breaks, any such time exceeding regularly scheduled and paid break time will be unpaid.

Members desiring to take a lactation break shall notify the dispatcher or a supervisor prior to taking such a break. Such breaks may be reasonably delayed if they would seriously disrupt department operations.

Once a lactation break has been approved, the break should not be interrupted except for emergency or exigent circumstances.

1017.4 PRIVATE LOCATION

The Department will make reasonable efforts to accommodate members with the use of an appropriate room or other location to express milk in private. Such room or place should be in proximity to the member’s work area and shall be other than a bathroom or toilet stall. The location must be shielded from view and free from intrusion from co-workers and the public (29 USC § 207; Va. Code § 2.2-3904).

Members occupying such private areas shall either secure the door or otherwise make it clear to others that the area is occupied with a need for privacy. All other members should avoid interrupting a member during an authorized break, except to announce an emergency or other urgent circumstance.

Authorized lactation breaks for members assigned to the field may be taken at the nearest appropriate private area.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1017.5 STORAGE OF EXPRESSED MILK

Any member storing expressed milk in any authorized refrigerated area within the Department shall clearly label it as such and shall remove it when the member’s shift ends.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Payroll Records

1018.1 PURPOSE AND SCOPE

This policy provides the guidelines for completing and submitting payroll records of department members who are eligible for the payment of wages.

1018.2 POLICY

The Madison County Sheriff's Office maintains timely and accurate payroll records.

1018.3 RESPONSIBILITIES

Members are responsible for the accurate completion and timely submission of their payroll records for the payment of wages.

Supervisors are responsible for approving the payroll records for those under their commands.

1018.4 TIME REQUIREMENTS

Members who are eligible for the payment of wages are paid on a scheduled, periodic basis, generally on the same day or date each period, with certain exceptions, such as holidays. Payroll records shall be completed and submitted to Administration as established by the County payroll procedures.

1018.5 RECORDS

The Administration Division Supervisor shall ensure that accurate and timely payroll records are maintained as required by 29 CFR 516.2 for a minimum of three years (29 CFR 516.5).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Overtime Compensation

1019.1 PURPOSE AND SCOPE

This policy establishes guidelines and procedures regarding overtime for employees, in conformance with the Fair Labor Standards Act (FLSA) (29 USC § 201 et seq.).

1019.2 POLICY

The Madison County Sheriff's Office will compensate nonexempt employees who work authorized overtime either by payment of wages or by the accrual of compensatory time (29 CFR 553.22). Employees who are salary exempt from FLSA are not compensated for overtime worked.

1019.3 COMPENSATION

Payment of wages to nonexempt employees for overtime, or accrual of compensatory time in lieu of compensation for overtime worked, shall be at the rate of not less than one and one-half hours for each hour of employment for which overtime compensation is required (29 USC § 207(k)(2); 29 USC § 207(o)(1); Va. Code § 9.1-701; Va. Code § 40.1-29.2).

Short periods of overtime worked at the end of the normal duty day (e.g., less than one hour in duration) may be handled informally by an agreement between the supervisor and the employee. In such cases, the supervisor shall document the overtime worked and schedule a subsequent shift adjustment within the same work period that the overtime was worked, rather than submit a request for overtime compensation (29 USC § 207(k)).

Salary exempt employees may be eligible for administrative leave, which may be granted at the discretion of the exempt employee’s immediate supervisor.

1019.4 REQUESTS FOR OVERTIME COMPENSATION

1019.4.1 EMPLOYEE RESPONSIBILITIES

Generally, no employee is authorized to work overtime without the prior approval of a supervisor. If circumstances do not permit prior approval, approval shall be sought as soon as practicable during the overtime shift and in no case later than the end of the shift in which the overtime is worked.

Nonexempt employees shall:

(a) Obtain supervisory approval, verbal or written.

(b) Not work in excess of 16 hours, including regularly scheduled work time, overtime and extra-duty time, in any consecutive 24-hour period without supervisory approval.

(c) Record the actual time worked in an overtime status using the department-approved form or method. Informal notations on reports, logs or other forms not approved for overtime recording are not acceptable.

(d) Submit the request for overtime compensation to their supervisors by the end of shift or no later than the next calendar day.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1019.4.2 SUPERVISOR RESPONSIBILITIES
Supervisors shall:

(a) Prior to authorizing an employee to work overtime, evaluate the need for overtime.
    1. Supervisors should not authorize any request to work overtime if the overtime would not be an appropriate use of department resources.

(b) Upon receipt of a request for overtime compensation, confirm that the overtime was authorized and then verify the actual time worked.
    1. Supervisors identifying any unauthorized overtime or discrepancy shall initiate an investigation consistent with the Personnel Complaints Policy.

(c) After verifying and approving the overtime amount, promptly forward the request for compensation to the employee's Division Supervisor for final approval.
    1. After the Division Supervisor has authorized compensation, the request shall be submitted to Administration as soon as practicable.

Supervisors may not authorize or approve their own overtime.

1019.5 ACCOUNTING FOR PORTIONS OF AN HOUR

Authorized overtime work shall be accounted in the increments as listed:

TIME WORKED	INDICATE ON CARD
Up to 15 minutes	.25 hour
16 to 30 minutes	.50 hour
31 to 45 minutes	.75 hour
46 to 60 minutes	1 hour

1019.5.1 VARIATION IN TIME REPORTED
When two or more employees are assigned to the same activity, case, or court trial, and the amount of time for which overtime compensation is requested varies among the deputies, the Shift Supervisor or other approving supervisor shall require each employee to include the reason for the variation on the overtime compensation request.

1019.6 REQUESTING USE OF COMPENSATORY TIME

Employees who have accrued compensatory time shall be allowed to use that time for time off within a reasonable period after making a request if the request does not unduly disrupt department operations. Requests to use compensatory time will be submitted to the employee's supervisor at least thirty days in advance of its intended use. Supervisors may make exceptions in unusual or extraordinary circumstances.

Compensatory time may not be used for time off for a date and time when the employee is required to appear in court on department-related matters. Supervisors shall not unreasonably deny employee requests to use compensatory time (29 CFR 553.25).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Outside Employment and Outside Overtime

1020.1 PURPOSE AND SCOPE

This policy provides guidelines for department members who seek to engage in authorized outside employment or outside overtime.

1020.1.1 DEFINITIONS

Definitions related to this policy include:

Outside employment - Duties or services performed by members of this department for another employer, organization or individual who is not affiliated directly with this department when wages, compensation or other consideration for such duties or services is received. Outside employment also includes duties or services performed by those members who are self-employed and receive compensation or other consideration for services, products or benefits rendered.

Outside overtime - Duties or services performed by members of this department for a private organization, entity or individual, that are requested and scheduled directly through the Department. Member compensation, benefits and costs for such outside services are reimbursed to the Department.

1020.2 POLICY

Members of the Madison County Sheriff's Office shall obtain written approval from the Sheriff or the authorized designee prior to engaging in any outside employment or outside overtime. Approval of outside employment or overtime shall be at the discretion of the Sheriff in accordance with the provisions of this policy. Failure to obtain prior written approval for outside employment or overtime, or engaging in outside employment or overtime that is prohibited by this policy, may lead to disciplinary action.

1020.2.1 POINT OF COORDINATION

The Sheriff or the authorized designee will act as the point of coordination for outside employment and outside overtime to oversee adherence to department policies and procedures.

1020.3 OUTSIDE EMPLOYMENT

1020.3.1 DENIAL

Any member whose request for outside employment has been denied should be provided with a written notification of the reason at the time of the denial.

1020.3.1 REQUEST AND APPROVAL

Members must submit the designated outside employment request form to his/her immediate supervisors. The request form will then be forwarded through the chain of command to the Sheriff for consideration.

If approved, the member will be provided with a copy of the approved request form. Unless otherwise indicated in writing on the request form, approval for outside employment will be valid

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

through the end of the calendar year in which the request is approved. Members seeking to continue outside employment must submit a new request form at the start of each calendar year.

1020.3.2 REVOCATION OR SUSPENSION
Any member whose approval for outside employment is revoked or suspended should be provided with a written notification of the reason for revocation or suspension.

Approval for outside employment may be revoked or suspended:

(a) When a supervisor determines the member’s performance is failing to meet standards and the outside employment may be related to the deficient performance.

    1. Approval for the outside employment may be reestablished when the member’s performance has reached a satisfactory level and with his/her supervisor’s authorization.

(b) When a member’s conduct or outside employment conflicts with department policy or any law.

(c) When the outside employment creates an actual or apparent conflict of interest with the Department or County.

1020.3.3 APPEAL
If a member's request for outside employment is denied or if previous approval is revoked or suspended, the member may file a written notice of appeal with the Sheriff within 10 days of receiving notice of the denial, revocation or suspension.

A revocation or suspension will only be implemented after the member has completed the appeal process.

If the member's appeal is denied, he/she may file a grievance as provided in the Grievances Policy.

1020.4 REQUIREMENTS

1020.4.1 PROHIBITED OUTSIDE EMPLOYMENT
The Department reserves the right to deny any request for outside employment that involves:

(a) The use of department time, facilities, equipment or supplies.

(b) The use of the Madison County Sheriff's Office badge, uniform or influence for private gain or advantage.

(c) The member’s receipt or acceptance of any money or other consideration for the performance of duties or services that he/she would be required or expected to render in the course or hours of his/her employment, appointment or as a part of his/her regular duties.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) The performance of duties or services that may later be subject directly or indirectly to the control, inspection, review, audit or enforcement of any other member of this department.

(e) Demands upon the member’s time that would render the performance of his/her duties for this department deficient or substandard.

(f) Activities that may conflict with any other policy or rule of the Department (Va. Code § 15.2-1712).

(g) Activities which may occasionally require the use of the member's police powers in the performance of such employment that are not authorized by local ordinance (Va. Code § 15.2-1712).

1020.4.2 SECURITY AND LAW ENFORCEMENT OFFICER OUTSIDE EMPLOYMENT

No member of this department may engage in any outside employment as a law enforcement officer, private security guard, private investigator or other similar private security position without the written approval of the Sheriff.

1020.4.3 DEPARTMENT RESOURCES

Members are prohibited from using any department equipment or resources in the course of, or for the benefit of, any outside employment. This shall include the prohibition against any member using his/her position with this department to gain access to official records or databases of this department or other agencies.

1020.4.4 REVIEW OF FINANCIAL RECORDS

Prior to approving outside employment, the Department may request that a member provide his/her personal financial records for review if the Sheriff determines that a conflict of interest may exist. Failure or refusal by the member to provide such records may result in denial of the outside employment.

If, after approving a request for outside employment, the Department obtains information that a financial conflict of interest exists, the Department may request that the member provide his/her personal financial records for review. Failure or refusal by the member to provide such records may result in revocation or suspension of approval of the outside employment pursuant to this policy.

1020.4.5 CHANGES IN OUTSIDE EMPLOYMENT STATUS

If a member terminates his/her outside employment, the member shall promptly submit written notification of such termination to the Sheriff through the chain of command. Any subsequent request for renewal or continued outside employment must thereafter be processed and approved through the procedures set forth in this policy.

Members shall also promptly submit in writing to the Sheriff any material changes in outside employment, including any change in the number of hours, type of duties or the demands of any approved outside employment. Members who are uncertain whether a change in outside employment is material are advised to report the change.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1020.4.6 LEAVE OR RESTRICTED DUTY STATUS

Members who are placed on leave or other restricted duty status shall inform their immediate supervisors in writing within five days as to whether they intend to continue their outside employment while on such leave or restricted status. The immediate supervisor shall review the duties of the outside employment, along with any related orders (e.g., administrative, medical), and make a recommendation to the Sheriff regarding whether such employment should continue.

In the event that the Sheriff determines that the outside employment should be discontinued, or if the member fails to promptly notify his/her supervisor of his/her intention regarding outside employment, a notice revoking approval of the outside employment will be forwarded to the member and a copy attached to the original outside employment request form.

Criteria for revoking approval due to leave or restricted duty status include, but are not limited to:

(a) The outside employment is medically detrimental to the total recovery of the disabled member, as indicated by the County's medical professional advisers.

(b) The outside employment requires performance of the same or similar physical ability as would be required of an on-duty member.

(c) The member’s failure to make timely notice of his/her intention to the supervisor.

When the member returns to full duty with the Madison County Sheriff's Office, a written request may be submitted to the Sheriff to approve the outside employment request.

1020.5 OUTSIDE OVERTIME

1020.5.1 REQUESTS FOR SPECIAL SERVICES

Any private organization, entity or individual seeking special services (e.g., security, traffic control) from members of this department must submit a written request to the Sheriff in advance of the desired service. Such services will be assigned, monitored and compensated through the Department as outside overtime assignments.

(a) A request for special services during or at the site of a strike, lockout, picket or other physical demonstration of a labor dispute will not be approved.

(b) The requester will be required to enter into an agreement that includes indemnification with the Department prior to approval.

(c) The requester will be required to reimburse the Department for the members' compensation, benefits and costs (e.g., court time) associated with such outside services.

(d) Should such a request be approved, any member working outside overtime shall be subject to the following conditions:

1. The member shall wear the department uniform and carry department identification.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. The member shall be subject to the rules and regulations of this department.
3. Compensation for such approved outside overtime shall be pursuant to normal overtime procedures (see the Overtime Compensation Policy).
4. Outside overtime shall not be subject to the employment agreement.

(e) Outside overtime shall be assigned at the discretion of the Sheriff or as directed by county rule or policy.

1020.5.2 ARREST AND REPORTING PROCEDURE

Any deputy making an arrest or taking other official law enforcement action while working in an outside overtime assignment shall be required to complete all related reports in a timely manner pursuant to the Report Preparation Policy. Time spent on the completion of such reports shall be considered part of the outside overtime assignment.

1020.5.3 SPECIAL RESTRICTIONS

Except for emergency situations or with prior authorization from the Division Supervisor, undercover deputies or deputies assigned to covert operations shall not be eligible to work outside overtime in a uniformed or other capacity that could reasonably disclose the deputy's law enforcement status.

1020.5.4 REVOCATION OF OUTSIDE OVERTIME

In the event that the Sheriff determines that a member's participation in outside overtime should be discontinued, a notice will be forwarded to the member.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Work-Related Disease, Injury, and Death Reporting

1021.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance regarding timely reporting of work-related injuries, mental health issues, occupational diseases, and death.

1021.1.1 DEFINITIONS

Definitions related to this policy include:

Work-related injury - An accidental injury, occupational disease, or mental health issue arising out of and in the course of employment with the Madison County Sheriff's Office. An occupational disease does not include an ordinary disease of life to which the general public is exposed outside of the employment with the Madison County Sheriff's Office (Va. Code § 65.2-101; Va. Code § 65.2-107; Va. Code § 65.2-400).

1021.2 POLICY

The Madison County Sheriff's Office will address work-related injuries, occupational diseases and deaths appropriately, and will comply with applicable state workers' compensation requirements (Va. Code § 65.2-100 et seq.).

1021.3 RESPONSIBILITIES

See attachment: SUPERVISORS REPORT OF EMPLOYEE ACCIDENT.pdf

See attachment: EMPLOYEE ACCIDENT REPORT.pdf

See attachment: Madison County 2020 Co Nurse.pdf

See attachment: ACCIDENT WITNESS STATEMENT.pdf

1021.3.1 MEMBER RESPONSIBILITIES

Any member sustaining any occupational disease or work-related injury shall report such event as soon as practicable, but within 24 hours to a supervisor, and shall seek medical care when appropriate.

1021.3.2 SUPERVISOR RESPONSIBILITIES

A supervisor learning of any work-related injury or occupational disease should ensure the member receives medical care as appropriate.

Supervisors shall ensure that required documents regarding workers' compensation are completed and forwarded promptly. Any related County-wide injury- or illness-reporting protocol shall also be followed.

Supervisors shall determine whether the Major Incident Notification and Illness and Injury Prevention policies apply and take additional action as required.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1021.3.3 DIVISION SUPERVISOR RESPONSIBILITIES
The Division Supervisor who receives a report of an occupational disease or work-related injury should review the report for accuracy and determine what additional action should be taken. The report shall then be forwarded to the Sheriff, the County's risk management entity and the Administration Division Supervisor to ensure any required Virginia Occupational Safety and Health (VOSH) Program reporting is made as required in the illness and injury prevention plan identified in the Illness and Injury Prevention Policy.

1021.3.4 SHERIFF RESPONSIBILITIES
The Sheriff shall review and forward copies of the report to the Human Resources Department. Copies of the report and related documents retained by the Department shall be filed in the member's confidential medical file.

1021.4 OTHER DISEASE OR INJURY
Diseases and injuries caused or occurring on-duty that do not qualify for workers' compensation reporting shall be documented on the designated report of injury form, which shall be signed by a supervisor. A copy of the completed form shall be forwarded to the appropriate Division Supervisor through the chain of command and a copy sent to the Administration Division Supervisor.

Unless the injury is extremely minor, this report shall be signed by the affected member, indicating that he/she desired no medical attention at the time of the report. By signing, the member does not preclude his/her ability to later seek medical attention.

1021.5 SETTLEMENT OFFERS
When a member sustains an occupational disease or work-related injury that is caused by another person and is subsequently contacted by that person, his/her agent, insurance company or attorney and offered a settlement, the member shall take no action other than to submit a written report of this contact to his/her supervisor as soon as possible.

1021.5.1 NO SETTLEMENT WITHOUT PRIOR APPROVAL
No less than 10 days prior to accepting and finalizing the settlement of any third-party claim arising out of or related to an occupational disease or work-related injury, the member shall provide the Sheriff with written notice of the proposed terms of such settlement. In no case shall the member accept a settlement without first providing written notice to the Sheriff. The purpose of such notice is to permit the County to determine whether the offered settlement will affect any claim the County may have regarding payment for damage to equipment or reimbursement for wages against the person who caused the illness or injury, and to protect the County's right of subrogation, while ensuring that the member's right to receive compensation is not affected.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Personal Appearance Standards

1022.1 PURPOSE AND SCOPE

This policy provides guidelines for the personal appearance of members of the Madison County Sheriff's Office.

Requirements for department uniforms and civilian attire are addressed in the Uniforms and Civilian Attire Policy.

1022.2 POLICY

Madison County Sheriff's Office members shall maintain their personal hygiene and appearance to project a professional image that is appropriate for this department and for their assignments. Department personal appearance standards are primarily based on safety requirements, appearance conformity and the social norms of the community served, while considering matters important to members of the Department.

1022.3 GROOMING

Unless otherwise stated and because deviations from these standards may present officer safety issues, the following appearance standards shall apply to all members, except those whose current assignments would deem them not applicable, and where the Sheriff has granted an exception.

1022.3.1 PERSONAL HYGIENE

All members must maintain proper personal hygiene. Examples of improper personal hygiene include, but are not limited to, dirty fingernails, bad breath, body odor and dirty or unkempt hair. Any member who has a condition due to a protected category (e.g., race, physical disability) that affects any aspect of personal hygiene covered by this policy may qualify for an accommodation and should report any need for an accommodation to the Sheriff.

1022.3.2 HAIR

Hair shall be clean, neatly trimmed or arranged, and of a natural hair color. Hairstyles with shaved designs in the scalp are prohibited. Hair adornments shall be primarily for the purpose of securing the hair and must present a professional image.

Hairstyles for male department members must not extend below the top edge of a uniform or dress shirt collar while assuming a normal stance.

When working a field assignment, hairstyles for female department members must not extend below the bottom edge of a uniform or dress shirt collar while assuming a normal stance. Longer hair shall be worn up or in a tightly wrapped braid or ponytail that is secured to the head above the bottom edge of the shirt collar.

1022.3.3 MUSTACHES

Mustaches shall not extend below the corners of the mouth or beyond the natural hairline of the upper lip and shall be short and neatly trimmed.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1022.3.4 SIDEBURNS
Sideburns shall not extend below the bottom of the outer ear opening (the top of the earlobes) and shall be trimmed and neat.

1022.3.5 FACIAL HAIR
Facial hair, other than sideburns, mustaches and eyebrows, is prohibited, unless authorized by the Sheriff or the authorized designee.

1022.3.6 FINGERNAILS
Fingernails shall be clean and neatly trimmed to a length that will not present a safety concern. The color of fingernail polish shall present a professional image.

1022.4 APPEARANCE

1022.4.1 JEWELRY
For the purpose of this policy, jewelry refers to rings, earrings, necklaces, bracelets, wristwatches, and tie tacks or tie bars. Jewelry shall present a professional image and may not create a safety concern for the department member or others. Jewelry that depicts racial, sexual, discriminatory, gang-related, or obscene language is not allowed.

(a) Necklaces shall not be visible above the shirt collar.

(b) Earrings shall be small and worn only in or on the earlobe.

(c) One ring or ring set may be worn on each hand of the department member. No rings should be of the type that would cut or pose an unreasonable safety risk to the member or others during a physical altercation, if the member is assigned to a position where that may occur.

(d) One small bracelet, including a bracelet identifying a medical condition, may be worn on one arm.

(e) Wristwatches shall be conservative and present a professional image.

(f) Tie tacks or tie bars worn with civilian attire shall be conservative and present a professional image.

1022.4.2 TATTOOS
While on-duty or representing the Madison County Sheriff's Office in any official capacity, members should make every reasonable effort to conceal tattoos or other body art. At no time while the member is on-duty or representing the Department in any official capacity shall any offensive tattoo or body art be visible. Examples of offensive tattoos include but are not limited to those that exhibit or advocate discrimination; those that exhibit gang, supremacist, or extremist group affiliation; and those that depict or promote drug use, sexually explicit acts, or other obscene material.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1022.4.3 BODY PIERCING OR ALTERATION

Body piercing (other than earlobes) or alteration to any area of the body that is visible while on-duty or while representing the Madison County Sheriff's Office in any official capacity, that is a deviation from normal anatomical features and that is not medically required, is prohibited. Such body alteration includes, but is not limited to:

(a) Tongue splitting or piercing.

(b) The complete or transdermal implantation of any material other than hair replacement (i.e., foreign objects inserted under the skin to create a design or pattern).

(c) Abnormal shaping of the ears, eyes, nose or teeth (i.e., enlarged or stretched out holes in the earlobes).

(d) Branding, scarification or burning to create a design or pattern.

1022.4.4 DENTAL ORNAMENTATION

Dental ornamentation that is for decorative purposes and that is not medically required is prohibited while on-duty or while representing the Madison County Sheriff's Office in any official capacity. Such ornamentation includes, but is not limited to:

(a) Objects that are bonded to front teeth.

(b) Gold, platinum or other veneers or caps used for decorative purposes.

(c) Orthodontic appliances that are colored for decorative purposes.

1022.4.5 GLASSES AND CONTACT LENSES

Eyeglasses and sunglasses shall be conservative and present a professional image. Contact lenses with designs that change the normal appearance of the eye and that are not medically required are prohibited while on-duty or while representing the Madison County Sheriff's Office in any official capacity.

1022.4.6 COSMETICS AND FRAGRANCES

Cosmetics shall be conservative and present a professional image. Use of cologne, perfume, aftershave lotion and other items used for body fragrance shall be kept to a minimum.

1022.4.7 UNDERGARMENTS

Proper undergarments shall be worn as necessary for reasons of hygiene and general appearance standards.

1022.5 RELIGIOUS ACCOMMODATION

The religious beliefs and needs of department members should be reasonably accommodated. Requests for religious accommodation should generally be granted unless there is a compelling security or safety reason and denying the request is the least restrictive means available to ensure security or safety. The Sheriff should be advised any time a request for religious accommodation is denied.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Personal Appearance Standards

Those who request to wear headscarves, simple head coverings, certain hairstyles, or facial hair for religious reasons should generally be accommodated absent unusual circumstances.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Uniforms and Civilian Attire

1023.1 PURPOSE AND SCOPE

This policy provides guidelines for Madison County Sheriff's Office-authorized uniforms and civilian attire regulations. It is established to ensure that uniformed members will be readily identifiable to the public through the proper use and wearing of department uniforms, and that the appearance of members who wear civilian attire reflects favorably on the Department.

This policy addresses the wearing and maintenance of department uniforms, accessories, insignia, patches and badge; the requirements for members who wear civilian attire; and the authorized use of optional equipment and accessories by members of the Department.

Other related topics are addressed in the Badges, Patches and Identification, Department-Owned and Personal Property, and Personal Appearance Standards policies.

1023.2 POLICY

The Madison County Sheriff's Office will provide uniforms for all employees who are required to wear them in the manner, quantity and frequency as determined by the Sheriff or the authorized designee. The Department may provide other department members with uniforms at the direction of the Sheriff.

All uniforms and equipment issued to department members shall be returned to the Department upon termination or resignation.

1023.3 UNIFORMS

The Sheriff or the authorized designee shall maintain and update uniform and equipment specifications, which should be consulted by all members as needed. Uniforms shall be worn as described therein and as specified in this policy and in compliance with Va. Code § 19.2-78 and Va. Code § 46.2-102.

The following shall apply to those assigned to wear department-issued uniforms:

(a) Uniforms and equipment shall be maintained in a serviceable condition and shall be ready at all times for immediate use. Uniforms shall be neat, clean and appear professionally pressed.

(b) Deputies in a non-uniformed assignment shall possess and maintain at all times a serviceable uniform and the necessary equipment to perform uniformed field duty.

(c) Uniforms shall be worn in compliance with any applicable department specifications.

(d) Members shall wear only the uniforms specified for their ranks and assignments.

(e) Civilian attire shall not be worn in combination with any distinguishable part of a uniform.

(f) Uniforms are only to be worn while on-duty, for court, at official department functions or events, while in transit to or from work, or when authorized by the Sheriff or the authorized designee.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1. When the uniform is worn while in transit, a non-uniform outer garment shall be worn over the uniform shirt to avoid bringing attention to the member while he/she is off-duty.

(g) Members are not to purchase or drink alcoholic beverages while wearing any part of department-issued uniforms, including the uniform pants.

(h) All supervisors will perform periodic inspections of members under their commands to ensure conformance to this policy.

1023.3.1 ACCESSORIES

Members shall adhere to the following when wearing department uniforms:

(a) Mirrored sunglasses will not be worn.

(b) Jewelry shall be in accordance with the specifications in the Personal Appearance Standards Policy.

1023.3.2 INSIGNIA, PATCHES AND BADGE

Only the following elements may be affixed to department uniforms unless an exception is authorized by the Sheriff:

(a) Shoulder patch - The authorized shoulder patch supplied by the Department shall be machine stitched to the sleeves of all uniform shirts and jackets.

(b) Badge - The department-issued badge, or an authorized sewn-on cloth replica, must be worn and visible at all times while in uniform.

(c) Nameplate - The regulation nameplate, or an authorized sewn-on cloth nameplate, shall be worn at all times while in uniform.

1. When a jacket is worn, the nameplate, or an authorized sewn-on cloth nameplate, shall be affixed to the jacket in the same manner as the uniform.

(d) Rank insignia - The designated insignia indicating the member's rank must be worn at all times while in uniform.

(e) Service insignia - The designated insignia indicating the member's length of service may be worn on long-sleeve shirts and jackets. The insignia shall be machine stitched to the left sleeve of the uniform.

(f) Assignment insignias - Assignment insignias (e.g., Crisis Response Unit CRU, Field Training Officer (FTO)) may be worn as designated by the Sheriff.

(g) American flag pin - An American flag pin may be worn, centered above the nameplate.

(h) Award/commendation insignia - Insignia representing an award or commendation received under the Commendations and Awards Policy, or other recognition authorized by the Sheriff, may be worn, centered above the nameplate. If more than one award is worn, or an American flag pin is worn, the insignia shall be equally spaced in one or two horizontal rows centered above the nameplate in a manner that provides a balanced appearance.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1023.3.3 MOURNING BAND

Uniformed members shall wear a black mourning band across the department badge whenever a law enforcement officer is killed in the line of duty or as directed by the Sheriff. The following mourning periods will be observed:

(a) Madison County Sheriff's Office deputy - From the time of death until midnight on the 14th day after the death.

(b) A deputy from this or an adjacent county - From the time of death until midnight on the day of the funeral.

(c) Funeral attendee - While attending the funeral of an out-of-region fallen officer.

(d) National Peace Officers' Memorial Day (May 15) - From 0001 hours until 2359 hours.

(e) As directed by the Sheriff.

1023.4 UNIFORM CLASSES

The Sheriff or the authorized designee shall determine the uniform to be worn by each department member or any deviations that may be authorized.

Uniforms are classified as follows:

(a) Class A - Full dress uniform to be worn by designated department members on special occasions, such as funerals, graduations, ceremonies, or as directed by the Sheriff or the authorized designee.

(b) Class B - Standard issue uniform to be worn daily by designated department members.

(c) Class C - General utility uniform to be worn by designated Department members.

(d) Specialized assignment - Specific uniforms to be worn by members in special assignments or divisions.

1023.4.1 CLASS A UNIFORM

The Class A uniform consists of the following:

(a) Long-sleeve shirt

(b) Tie tack or tie bar

(c) Trousers or skirt

(d) Black belt

1. Belts shall be equipped as needed for the member's assignment.

(e) Dark blue or black socks

1. Natural colored hose must be worn with the skirt.

(f) Black polished dress shoes

1. Boots with pointed toes are not permitted.

(g) White gloves

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1023.4.2 CLASS B UNIFORM
The Class B uniform consists of the following:

(a) Long- or short-sleeve shirt with the collar open and no tie
    1. A crew neck t-shirt must be worn under the uniform shirt.
    2. All shirt buttons must remain buttoned except for the top button at the neck.
    3. Long sleeves must be buttoned at the cuff.
(b) Trousers or skirt
(c) Black belt
    1. Belts shall be equipped as needed for the member’s assignment.
(d) Dark blue or black socks
    1. Natural colored hose must be worn with the skirt.
(e) Black polished dress shoes
    1. Approved black unpolished shoes may be worn.
    2. Boots with pointed toes are not permitted.
    3. Decorative stitching or adornment is not permitted.
(f) Weather-appropriate items
    1. Hat
    2. Dark blue or black mock turtleneck may be worn under the long-sleeve uniform shirt
    3. Jacket
    4. Rain gear

1023.4.3 CLASS C UNIFORM
The Sheriff or the authorized designee will establish the specifications, regulations and conditions for wearing the Class C uniform.

1023.4.4 SPECIALIZED ASSIGNMENT UNIFORM
The Sheriff or the authorized designee may authorize certain uniforms to be worn by members in specialized assignments, such as canine handlers, the (CRU), bicycle patrol, motor deputies and other specific assignments.

1023.5 CIVILIAN ATTIRE
There are assignments within the Department that do not require a uniform because recognition and authority are not essential to their functions. There are also assignments for which civilian attire is necessary.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) Civilian attire shall fit properly, be clean and free of stains, and not be damaged or excessively worn.

(b) Members assigned to administrative, investigative and support positions shall wear business-appropriate clothing that is conservative in style.

(c) Variations from this policy are allowed at the discretion of the Sheriff or the authorized designee when the member's assignment or current task is not conducive to wearing such clothing.

(d) No item of civilian attire may be worn while on-duty that would adversely affect the reputation of the Madison County Sheriff's Office or the morale of the members.

(e) The following items shall not be worn while on-duty or when representing the Department in any official capacity:

1. Clothing that reveals cleavage, the back, chest, stomach or buttocks
2. T-shirt alone or exposed undergarments
3. Swimsuits, tank tops, tube tops or halter tops
4. Sweatshirts, sweatpants or similar exercise clothing
5. Spandex-type pants or transparent clothing
6. Denim pants of any color
7. Shorts
8. Open-toed shoes
9. Clothing, buttons or pins displaying racial, sexual, discriminatory, gang-related or obscene language

1023.6 OPTIONAL EQUIPMENT

Any items that are allowed by the Madison County Sheriff's Office but that have been identified as optional shall be purchased entirely at the expense of the member. No part of the purchase cost shall be offset by the Department.

Maintenance of optional items shall be the financial responsibility of the purchasing member (e.g., repairs due to normal wear and tear).

Replacement of items listed in this policy as optional shall be managed as follows:

(a) When the item is no longer functional because of normal wear and tear, the member bears the full cost of replacement.

(b) When the item is no longer functional because of damage in the course of the member’s duties, it shall be replaced in accordance with the Department-Owned and Personal Property Policy.

1023.7 UNAUTHORIZED UNIFORMS, EQUIPMENT AND ACCESSORIES

Madison County Sheriff's Office members may not wear any uniform item, accessory or attachment unless specifically authorized by the Sheriff or the authorized designee.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Uniforms and Civilian Attire

Department members may not use or carry any safety item, tool or other piece of equipment unless specifically authorized by the Sheriff or the authorized designee.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Conflict of Interest

1024.1 PURPOSE AND SCOPE

The purpose of this policy is to assist members in recognizing and avoiding potential conflicts of interest, thereby ensuring effective and ethical operating practices on the part of the Madison County Sheriff's Office.

1024.1.1 DEFINITIONS

Definitions related to this policy include:

Conflict of interest - Any actual, perceived or potential conflict, in which it reasonably appears that a member's action, inaction or decisions are or may be influenced by a personal or business relationship.

1024.2 POLICY

Members of the Madison County Sheriff's Office are expected to conduct themselves with the utmost professional integrity and objectivity. Members will guard against actual or perceived conflicts of interest in order to ensure the fair and equitable treatment of department members and the public, and thereby maintain the trust of the public and department members.

1024.3 PROHIBITIONS

The Department prohibits the following types of personal or business relationships among members:

(a) Members are prohibited from directly supervising, occupying a position in the line of supervision or being directly supervised by any other member who is a relative or with whom they are involved in a personal or business relationship.

1. If circumstances require that such a supervisor/subordinate relationship exist temporarily, the supervisor shall make every reasonable effort to defer matters pertaining to the involved member to an uninvolved supervisor.

2. When personnel and circumstances permit, the Department will attempt to make every reasonable effort to avoid placing members in such supervisor/ subordinate situations. The Department, however, reserves the right to transfer or reassign any member to another position within the same classification in order to avoid conflicts with any provision of this policy.

(b) Members are prohibited from participating in, contributing to or recommending promotions, assignments, performance evaluations, transfers or other personnel decisions affecting a member who is a relative or with whom they are involved in a personal or business relationship.

(c) Whenever possible, field training officers (FTOs) and other trainers will not be assigned to train relatives. Department FTOs and other trainers are prohibited from entering into or maintaining personal or business relationships with any member they are assigned to train until such time as the training has been successfully completed and the person is off probation.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1024.4 MEMBER RESPONSIBILITIES

Members shall avoid situations that create a conflict of interest. Members should take reasonable steps to address a perception of a conflict of interest when such a perception is reasonably foreseeable and avoidable (e.g., deferring a decision to an uninvolved member) (Va. Code § 2.2-3103).

Whenever any member is placed in circumstances that would require him/her to take enforcement action or to provide official information or services to any relative or individual with whom the member is involved in a personal or business relationship, that member shall promptly notify his/her uninvolved, immediate supervisor.

In the event that no uninvolved supervisor is immediately available, the member shall promptly notify the dispatcher to have another uninvolved member either relieve the involved member or, minimally, remain present to witness the action.

1024.5 SUPERVISOR RESPONSIBILITIES

Upon being notified of or otherwise becoming aware of any circumstance that could result in or constitute an actual or potential violation of this policy, a supervisor shall take all reasonable steps to promptly mitigate or avoid such violations whenever possible. Supervisors shall also promptly notify the Sheriff or the authorized designee of such actual or potential violations through the chain of command.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Badges, Patches, and Identification

1025.1 PURPOSE AND SCOPE

The Madison County Sheriff's Office (MCSO) badge, patch, and identification card, as well as the likeness of these items and the name of the Department, are property of the Department. Their use shall be restricted as set forth in this policy.

1025.2 POLICY

The Madison County Sheriff's Office issues each member appropriate identification, which may include a badge, patch, and/or identification card, depending on the member's position within the Department.

1025.3 MEMBER RESPONSIBILITIES

Members of the Madison County Sheriff's Office will use the MCSO badge, patch, and identification card, as well as the likeness of these items, appropriately and professionally. The MCSO badge, patch, and identification card shall only be displayed or used by a member when acting in an official or authorized capacity.

Department members shall not:

(a) Display or use the MCSO badge, patch, or identification card for personal gain or benefit.

(b) Loan the MCSO badge, patch, or identification card to others or permit these items to be reproduced or duplicated.

(c) Use images of the MCSO badge, patch, or identification card, or the likeness thereof, or the Madison County Sheriff's Office name, for personal or private reasons including, but not limited to, letters, memoranda, and electronic communications, such as email, blogs, social networking, or websites.

1025.3.1 LOST BADGE, PATCH OR IDENTIFICATION CARD

Department members shall promptly notify their supervisors whenever their MCSO badges, patches or identification cards are lost, damaged or are otherwise removed from their control.

1025.4 BADGES

The Sheriff shall determine the number and form of badges authorized for use by department members.

Only badges issued by this department are authorized to be used, displayed, carried, or worn by members while on-duty or otherwise acting in an official or authorized capacity.

The placement and manner of display of the issued badge is addressed in the Uniforms and Civilian Attire Policy.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1025.4.1 RETIREE BADGES
The Sheriff or the authorized designee should provide retired deputies with their badge or other insignia, upon request, and issue it mounted in a manner that it cannot be displayed on the retired deputy (Va. Code § 9.1-1000).

1025.4.2 PERMITTED USE BY EMPLOYEE GROUPS
The likeness of the MCSO badge shall not be used for any purpose without the express authorization of the Sheriff and shall be subject to the following:

(a) An authorized employee group may use the likeness of the MCSO badge for merchandise and official employee group business provided it is used in a clear representation of the employee group and not the Madison County Sheriff's Office. The following modification shall be included:

1. Any text identifying the Madison County Sheriff's Office is replaced with the name of the employee group.

2. A badge number is not included. That portion of the badge may display the acronym of the employee group.

1025.5 IDENTIFICATION CARDS
All members will be issued an official MCSO identification card bearing the member's name, full-face photograph, member identification number, member's signature and signature of the Sheriff or the official seal of the Department. All members shall be in possession of their department-issued identification cards at all times while on-duty or in department facilities.

(a) Whenever on-duty or acting in an official capacity representing the Department, members shall display their department-issued identification cards in a courteous manner to any person upon request and as soon as practicable.

(b) Deputies or other members working specialized assignments may be excused from the possession and display requirements when directed by their Division Supervisors.

1025.6 BUSINESS CARDS
The Department will supply business cards to those members whose assignments involve frequent interaction with the public or who may require the use of a business card. The only authorized business cards are those issued or approved by the Department and should contain identifying information including, but not limited to, the member's name, division, badge or other identification number and contact information (e.g., telephone number, email address).

Members should provide a business card to any member of the public who requests one.

1025.7 LOST BADGE, PATCH, OR IDENTIFICATION CARD
Department members shall promptly notify their supervisors whenever their MCSO badges, patches, or identification cards are lost, damaged, or are otherwise removed from their control.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1025.8 PATCHES

The Sheriff shall determine the form of patches authorized for use by the Department. Any request to modify the authorized patches for specialty divisions (e.g., canine, SWAT) should be submitted to the Sheriff in writing.

Only patches issued by this department are authorized to be displayed or worn by members while on-duty or otherwise acting in an official or authorized capacity.

The placement and manner of display of the department-issued patch is addressed in the Uniforms and Civilian Attire Policy.

Members, with the written approval of the Sheriff, may request additional patches, at their own expense.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Temporary Modified-Duty Assignments

1026.1 PURPOSE AND SCOPE

This policy establishes procedures for providing temporary modified-duty assignments. This policy is not intended to affect the rights or benefits of employees under federal or state law, County rules, or policy. For example, nothing in this policy affects the obligation of the Department to engage in a good faith, interactive process to consider reasonable accommodations for any employee with a temporary or permanent disability that is protected under federal or state law.

1026.2 POLICY

Subject to operational considerations, the Madison County Sheriff's Office may identify temporary modified-duty assignments for employees who have an injury or medical condition resulting in temporary work limitations or restrictions. A temporary assignment allows the employee to work, while providing the Department with a productive employee during the temporary period.

1026.3 GENERAL CONSIDERATIONS

Priority consideration for temporary modified-duty assignments will be given to employees with work-related injuries or illnesses that are temporary in nature. Employees having disabilities covered under the Americans with Disabilities Act (ADA) or the Virginians with Disabilities Act shall be treated equally, without regard to any preference for a work-related injury.

No position in the Madison County Sheriff's Office shall be created or maintained as a temporary modified-duty assignment.

Temporary modified-duty assignments are a management prerogative and not an employee right. The availability of temporary modified-duty assignments will be determined on a case-by-case basis, consistent with the operational needs of the Department. Temporary modified-duty assignments are subject to continuous reassessment, with consideration given to operational needs and the employee's ability to perform in a modified-duty assignment.

The Sheriff or the authorized designee may restrict employees working in temporary modified-duty assignments from wearing a uniform, displaying a badge, carrying a firearm, operating an emergency vehicle or engaging in outside employment, or may otherwise limit them in employing their law enforcement officer powers.

Temporary modified-duty assignments shall generally not exceed a cumulative total of 1,040 hours in any one-year period.

1026.4 PROCEDURE

Employees may request a temporary modified-duty assignment for short-term injuries or illnesses.

Employees seeking a temporary modified-duty assignment should submit a written request to their Division Supervisors or the authorized designees. The request should, as applicable, include a certification from the treating medical professional containing:

(a) An assessment of the nature and probable duration of the illness or injury.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) The prognosis for recovery.

(c) The nature and scope of limitations and/or work restrictions.

(d) A statement regarding any required workplace accommodations, mobility aids, or medical devices.

(e) A statement that the employee can safely perform the duties of the temporary modified-duty assignment.

The Division Supervisor will make a recommendation through the chain of command to the Sheriff regarding temporary modified-duty assignments that may be available based on the needs of the Department and the limitations of the employee.

Requests for a temporary modified-duty assignment of 20 hours or less per week may be approved and facilitated by the Division Supervisor, with notice to the Sheriff.

1026.5 ACCOUNTABILITY

Written notification of assignments, work schedules and any restrictions should be provided to employees assigned to temporary modified-duty assignments and their supervisors. Those assignments and schedules may be adjusted to accommodate department operations and the employee's medical appointments, as mutually agreed upon with the Division Supervisor.

1026.5.1 EMPLOYEE RESPONSIBILITIES

The responsibilities of employees assigned to temporary modified duty shall include, but are not limited to:

(a) Communicating and coordinating any required medical and physical therapy appointments in advance with their supervisors.

(b) Promptly notifying their supervisors of any change in restrictions or limitations after each appointment with their treating medical professionals.

(c) Communicating a status update to their supervisors no less than once every 30 days while assigned to temporary modified duty.

(d) Submitting a written status report to the Division Supervisor that contains a status update and anticipated date of return to full duty when a temporary modified-duty assignment extends beyond 60 days.

1026.5.2 SUPERVISOR RESPONSIBILITIES

The employee's immediate supervisor shall monitor and manage the work schedule of those assigned to temporary modified duty.

The responsibilities of supervisors shall include, but are not limited to:

(a) Periodically apprising the Division Supervisor of the status and performance of employees assigned to temporary modified duty.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) Notifying the Division Supervisor and ensuring that the required documentation facilitating a return to full duty is received from the employee.

(c) Ensuring that employees returning to full duty have completed any required training and certification.

1026.6 MEDICAL EXAMINATIONS

Prior to returning to full-duty status, employees shall be required to provide certification from their treating medical professionals stating that they are medically cleared to perform the essential functions of their jobs without restrictions or limitations.

The Department may require a fitness-for-duty examination prior to returning an employee to full-duty status, in accordance with the Fitness for Duty Policy.

1026.7 PREGNANCY

If an employee is temporarily unable to perform regular duties due to a pregnancy, childbirth, or a related medical condition, the employee will be treated the same as any other temporarily disabled employee (42 USC § 2000e(k)). A pregnant employee shall not be involuntarily transferred to a temporary modified-duty assignment.

1026.7.1 NOTIFICATION

Pregnant employees should notify their immediate supervisors as soon as practicable and provide a statement from their medical providers identifying any pregnancy-related job restrictions or limitations. If at any point during the pregnancy it becomes necessary for the employee to take a leave of absence, such leave shall be granted in accordance with the County's personnel rules and regulations regarding family and medical care leave.

1026.8 PROBATIONARY EMPLOYEES

Probationary employees who are assigned to a temporary modified-duty assignment shall have their probation extended by a period of time equal to their assignment to temporary modified duty.

1026.9 MAINTENANCE OF CERTIFICATION AND TRAINING

Employees assigned to temporary modified duty shall maintain all certification, training and qualifications appropriate to both their regular and temporary duties, provided that the certification, training or qualifications are not in conflict with any medical limitations or restrictions. Employees who are assigned to temporary modified duty shall inform their supervisors of any inability to maintain any certification, training or qualifications.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Performance History Audits

1027.1 PURPOSE AND SCOPE

This policy provides guidance for the use of performance history audits. Performance history audits can help identify commendable performance as well as provide early recognition of training needs and other potential issues. This policy addresses the responsibilities, performance indicators and components of the audit, and handling of collected data.

1027.2 POLICY

The Madison County Sheriff's Office collects data to assist supervisors with evaluating the performance of their employees. While it is understood that the statistical compilation of data may be helpful to supervisors, the Department recognizes that it cannot account for, and must carefully balance such data with, the many variables in law enforcement, such as:

- Ability to detect crime.
- Work ethic.
- Assignment and shift.
- Physical abilities (ability to perform the job-related physical tasks).
- Randomness of events.

1027.3 RESPONSIBILITIES

Under the authority of the Administration Division Supervisor, the Internal Affairs Unit is responsible for collecting performance indicators and other relevant data. The data will be compiled to generate quarterly performance history audit reports that will be provided to the appropriate Division Supervisor. The Internal Affairs Unit will utilize confidential methods to compile and track information regarding performance indicators for each deputy during each quarter in order to prepare the report. Though generated quarterly, each report should contain data from a one-year time period.

The Administration Division Supervisor should forward a copy of each performance history audit report to the Sheriff for review and retention as confidential personnel information.

1027.4 COMPONENTS OF PERFORMANCE HISTORY AUDITS

Performance history audits should include the following components:

- Performance indicators
- Data analysis
- Employee review
- Follow-up monitoring

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Performance History Audits

1027.4.1 PERFORMANCE INDICATORS

Performance indicators represent the categories of employee performance activity that the Sheriff has determined may be relevant data for the generation and analysis of performance history audits. These indicators may include, but are not limited to, the frequency and/or number of:

(a) Use of force incidents.

(b) Involvement and conduct during vehicle pursuits.

(c) Personnel complaints, including the findings.

(d) Commendations, compliments, and awards from the Department and the public.

(e) Claims and civil suits related to the employee's actions or alleged actions.

(f) Canine bite incidents.

(g) Personnel investigations.

(h) Commonwealth Attorney case rejections and the reasons.

(i) Intentional or accidental firearm discharges (regardless of injury).

(j) Vehicle collisions.

(k) Missed court appearances.

(l) Documented counseling.

1027.4.2 DATA ANALYSIS

The Administration Division Supervisor will review each performance history audit report and determine whether it should be provided to the deputy’s immediate supervisor for further consideration.

1027.4.3 EMPLOYEE REVIEW

Upon receipt of a performance history audit report, the supervisor will carefully review the report with the deputy to assess any potential trends or other issues that may warrant informal counseling, additional training or a recommendation for other action, including discipline. The deputy shall date and sign the report and should be provided with a copy of the report upon request.

If a supervisor determines that a deputy's performance warrants action beyond informal counseling, the supervisor shall advise the Division Supervisor of such recommendation. If the Division Supervisor concurs with the recommendation of the supervisor, he/she shall take steps to initiate the appropriate action.

If discipline or other adverse action is initiated against a deputy as a result of a performance history audit, the deputy shall be entitled to all rights and processes set forth in the Personnel Complaints Policy.

1027.4.4 FOLLOW-UP MONITORING

Depending upon the results of each performance history audit, a determination should be made by the Administration Division Supervisor, after discussion with the deputy’s immediate supervisor,

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

about the need, type and duration of any follow-up. Performance indicators and data analysis will generally provide the basis upon which such decisions should be made.

1027.5 CONFIDENTIALITY OF DATA

Information, data and copies of material compiled to develop performance history audit reports shall be considered confidential as part of the employee's personnel file and will not be subject to discovery or release except as provided by law. Access to performance history audit reports will be governed under the same process as access to a deputy's personnel file, as outlined in the Personnel Records Policy.

Access to the underlying data will be governed by the process for access to the original records (such as police reports).

1027.6 RETENTION

Performance history audit reports and associated records shall be retained in accordance with the established records retention schedule.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Speech, Expression and Social Networking

1028.1 PURPOSE AND SCOPE

This policy is intended to address issues associated with the use of social networking sites, and provides guidelines for the regulation and balancing of member speech and expression with the needs of the Madison County Sheriff's Office.

This policy applies to all forms of communication including, but not limited to, film, video, print media, public or private speech and use of all Internet services, including the Web, email, file transfer, remote computer access, news services, social networking, social media, instant messaging, blogs, forums, video and other file-sharing sites.

Nothing in this policy is intended to prohibit or infringe upon any communication, speech or expression that is protected under law. This includes speech and expression protected under state or federal constitutions as well as labor or other applicable laws.

Members are encouraged to consult with their supervisors regarding any questions arising from the application or potential application of this policy.

1028.2 POLICY

Members of public entities occupy a trusted position in the community, and thus, their statements have the potential to contravene the policies and performance of the Madison County Sheriff's Office. Due to the nature of the work and influence associated with the law enforcement profession, it is necessary that members of this department be subject to certain reasonable limitations on their speech and expression. To achieve its mission and efficiently provide service to the public, the Department will carefully balance the individual member’s rights against the needs and interests of the Department when exercising a reasonable degree of control over its members’ speech and expression.

1028.3 SAFETY

Members should carefully consider the implications of their speech or any other form of expression when using the Internet. Speech and expression that may negatively affect the safety of Madison County Sheriff's Office members, such as posting personal information in a public forum or posting a photograph taken with a GPS-enabled camera, can result in compromising a member's home address or family ties. Members should therefore not disseminate or post any information on any forum or medium that could reasonably be anticipated to compromise the safety of any member, a member's family or associates. Examples of the type of information that could reasonably be expected to compromise safety include:

- Disclosing a photograph and name or address of a deputy who is working undercover.
- Disclosing the address of a fellow department member.
- Otherwise disclosing where another deputy can be located off-duty.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1028.4 PROHIBITED SPEECH, EXPRESSION AND CONDUCT

To meet the safety, performance and public-trust needs of the Madison County Sheriff's Office, the following are prohibited unless the speech is otherwise protected (for example, a member speaking as a private citizen on a matter of public concern):

(a) Speech or expression made pursuant to an official duty that tends to compromise or damage the mission, function, reputation or professionalism of the Department or its members.

(b) Speech or expression that, while not made pursuant to an official duty, is significantly linked to, or related to, the Department and tends to compromise or damage the mission, function, reputation or professionalism of the Department or its members. Examples may include:

1. Statements that indicate disregard for the law or the state or U.S. Constitutions.
2. Expression that demonstrates support for criminal activity.
3. Participation in sexually explicit photographs or videos for compensation or distribution.

(c) Speech or expression that could reasonably be foreseen as having a negative impact on the credibility of the member as a witness. For example, posting to a website statements or expressions that glorifies or endorses dishonesty, unlawful discrimination or illegal behavior.

(d) Speech or expression of any form that could reasonably be foreseen as having a negative impact on the safety of the members of the Department (e.g., a statement on a blog that provides specific details as to how and when prisoner transportations are made could reasonably be foreseen as potentially jeopardizing employees by informing criminals of details that could facilitate an escape or attempted escape).

(e) Speech or expression that is contrary to the canons of the Law Enforcement Code of Ethics as adopted by the Department.

(f) Use or disclosure, through whatever means, of any information, photograph, video or other recording obtained or accessible as a result of employment or appointment with the Department for financial or personal gain, or any disclosure of such materials without the express authorization of the Sheriff or the authorized designee.

(g) Posting, transmitting or disseminating any photographs, video or audio recordings, likenesses or images of department logos, emblems, uniforms, badges, patches, marked vehicles, equipment or other material that specifically identifies the Madison County Sheriff's Office on any personal or social networking or other website or web page, without the express authorization of the Sheriff.

Members must take reasonable and prompt action to remove any content, including content posted by others, that is in violation of this policy from any web page or website maintained by the employee (e.g., social or personal website).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1028.4.1 UNAUTHORIZED ENDORSEMENTS AND ADVERTISEMENTS

While members are not restricted from engaging in the following activities as private citizens, members may not represent the Madison County Sheriff's Office or identify themselves in any way that could be reasonably perceived as representing the Department in order to do any of the following, unless specifically authorized by the Sheriff:

(a) Endorse, support, oppose or contradict any political campaign or initiative.

(b) Endorse, support, oppose or contradict any social issue, cause or religion.

(c) Endorse, support or oppose any product, service, company or other commercial entity.

(d) Appear in any commercial, social or nonprofit publication or any motion picture, film, video or public broadcast or on any website.

Additionally, when it can reasonably be construed that an employee, acting in his/her individual capacity or through an outside group or organization, is affiliated with this department, the member shall give a specific disclaiming statement that any such speech or expression is not representative of the Madison County Sheriff's Office.

Members retain their rights to vote as they choose, to support candidates of their choice and to express their opinions as private citizens on political subjects and candidates at all times while off-duty. However, members may not use their official authority or influence to interfere with or affect the result of elections or nominations for office. Members are also prohibited from directly or indirectly using their official authority to coerce, command or advise another employee to pay, lend or contribute anything of value to a party, committee, organization, agency or person for political purposes (5 USC § 1502; Va. Code § 15.2-1512.2).

1028.5 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to emails, texts or anything published or maintained through file-sharing software or any Internet site (e.g., Facebook, Twitter, Instagram, etc.) that is accessed, transmitted, received or reviewed on any department technology system (see the Information Technology Use Policy for additional guidance).

1028.6 CONSIDERATIONS

In determining whether to grant authorization of any speech or conduct that is prohibited under this policy, the factors that the Sheriff or the authorized designee should consider include:

(a) Whether the speech or conduct would negatively affect the efficiency of delivering public services.

(b) Whether the speech or conduct would be contrary to the good order of the Department or the efficiency or morale of its members.

(c) Whether the speech or conduct would reflect unfavorably upon the Department.

(d) Whether the speech or conduct would negatively affect the member's appearance of impartiality in the performance of his/her duties.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(e) Whether similar speech or conduct has been previously authorized.

(f) Whether the speech or conduct may be protected and outweighs any interest of the Department.

1028.7 TRAINING

Subject to available resources, the Department should provide training regarding the limitations on speech, expression and use of social networking to all members of the Department.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Illness and Injury Prevention

1029.1 PURPOSE AND SCOPE

The purpose of this policy is to establish an ongoing and effective plan to reduce the incidence of illness and injury for members of the Madison County Sheriff's Office.

This policy specifically applies to illness and injury that results in lost time or that requires medical treatment beyond first aid. Although this policy provides the essential guidelines for a plan that reduces illness and injury, it may be supplemented by procedures outside the Policy Manual.

This policy does not supersede, but supplements any related County wide safety efforts.

1029.2 POLICY

The Madison County Sheriff's Office is committed to providing a safe environment for its members and visitors and to minimizing the incidence of work-related illness and injuries. The Department will establish and maintain an illness and injury prevention plan and will provide tools, training and safeguards designed to reduce the potential for accidents, injuries and illness. It is the intent of the Department to comply with all laws and regulations related to occupational safety.

1029.3 ILLNESS AND INJURY PREVENTION PLAN

The Administration Division Supervisor is responsible for developing an illness and injury prevention plan that shall include:

(a) Workplace safety and health training programs.

(b) Regularly scheduled safety meetings.

(c) Posted or distributed safety information.

(d) A system for members to anonymously inform management about workplace hazards.

(e) Establishment of a safety and health committee that will:

1. Meet regularly.
2. Prepare a written record of safety and health committee meetings.
3. Review the results of periodic scheduled inspections.
4. Review investigations of accidents and exposures.
5. Make suggestions to command staff for the prevention of future incidents.
6. Review investigations of alleged hazardous conditions.
7. Submit recommendations to assist in the evaluation of member safety suggestions.
8. Assess the effectiveness of efforts made by the Department to meet applicable standards (16 VAC 25-90-1910).

(f) Establishing a process to ensure illnesses and injuries are reported as required under the Virginia Occupational Safety and Health (VOSH) Program (Va. Code § 40.1-51.1; 16 VAC 25-85-1904).

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1029.4 ADMINISTRATION DIVISION SUPERVISOR RESPONSIBILITIES

The responsibilities of the Administration Division Supervisor include, but are not limited to:

(a) Managing and implementing a plan to reduce the incidence of member illness and injury.

(b) Ensuring that a system of communication is in place that facilitates a continuous flow of safety and health information between supervisors and members. This system shall include:

1. New member orientation that includes a discussion of safety and health policies and procedures.
2. Regular member review of the illness and injury prevention plan.

(c) Ensuring that all safety and health policies and procedures are clearly communicated and understood by all members.

(d) Taking reasonable steps to ensure that all members comply with safety rules in order to maintain a safe work environment. This includes, but is not limited to:

1. Informing members of the illness and injury prevention guidelines.
2. Recognizing members who perform safe work practices.
3. Ensuring that the member evaluation process includes member safety performance.
4. Ensuring department compliance to meet applicable standards (16 VAC 25-90-1910):
    (a) Exposure control mandates for bloodborne pathogens in 29 CFR 1910.1030
    (b) Personal Protective Equipment (PPE) (see the Personal Protective Equipment Policy) (29 CFR 1910.132)
    (c) Exit route, emergency action plans and fire prevention plans
    (d) Communicable diseases
    (e) Walking-Working surfaces (29 CFR 1910.21 et seq.)

(e) Making available a form to document inspections, unsafe conditions or unsafe work practices, and actions taken to correct unsafe conditions and work practices.

(f) Making available a form to document individual incidents or accidents.

(g) Making available a form to document the safety and health training of each member. This form will include the member’s name or other identifier, training dates, type of training and training providers.

(h) Conducting and documenting a regular review of the illness and injury prevention plan.

1029.5 SUPERVISOR RESPONSIBILITIES

Supervisor responsibilities include, but are not limited to:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(a) Ensuring member compliance with illness and injury prevention guidelines and answering questions from members about this policy.

(b) Training, counseling, instructing or making informal verbal admonishments any time safety performance is deficient. Supervisors may also initiate discipline when it is reasonable and appropriate under the Standards of Conduct Policy.

(c) Establishing and maintaining communication with members on health and safety issues. This is essential for an injury-free, productive workplace.

(d) Completing required forms and reports relating to illness and injury prevention; such forms and reports shall be submitted to the Administration Division Supervisor.

(e) Notifying the Administration Division Supervisor when:

1. New substances, processes, procedures or equipment that present potential new hazards are introduced into the work environment.
2. New, previously unidentified hazards are recognized.
3. Occupational illnesses and injuries occur.
4. New and/or permanent or intermittent members are hired or reassigned to processes, operations or tasks for which a hazard evaluation has not been previously conducted.
5. Workplace conditions warrant an inspection.

1029.6 HAZARDS

All members should report and/or take reasonable steps to correct unsafe or unhealthy work conditions, practices or procedures in a timely manner. Members should make their reports to a supervisor (as a general rule, their own supervisors).

Supervisors should make reasonable efforts to correct unsafe or unhealthy work conditions in a timely manner, based on the severity of the hazard. These hazards should be corrected when observed or discovered, when it is reasonable to do so. When a hazard exists that cannot be immediately abated without endangering members or property, supervisors should protect or remove all exposed members from the area or item, except those necessary to correct the existing condition.

Members who are necessary to correct the hazardous condition shall be provided with the necessary protection.

All significant actions taken and dates they are completed shall be documented on the appropriate form. This form should be forwarded to the Administration Division Supervisor via the chain of command.

The Administration Division Supervisor will take appropriate action to ensure the illness and injury prevention plan addresses potential hazards upon such notification.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1029.7 INSPECTIONS

Safety inspections are crucial to a safe work environment. These inspections identify and evaluate workplace hazards and permit mitigation of those hazards. A hazard assessment checklist should be used for documentation and to ensure a thorough assessment of the work environment.

The Administration Division Supervisor shall ensure that the appropriate documentation is completed for each inspection.

See attachment: Workplace Accident Investigation Form.pdf

See attachment: Workplace Safety Inspection Checklist.pdf

1029.7.1 EQUIPMENT

Members are charged with daily vehicle inspections of their assigned vehicles and of their PPE prior to working in the field. Members shall complete the appropriate form if an unsafe condition cannot be immediately corrected. Members should forward this form to their supervisors.

1029.8 INVESTIGATIONS

Any member sustaining any work-related illness or injury, as well as any member who is involved in any accident or hazardous substance exposure while on-duty, shall report such event as soon as practicable to a supervisor. Members observing or learning of a potentially hazardous condition are to promptly report the condition to their immediate supervisors.

A supervisor receiving such a report should personally investigate the incident or ensure that an investigation is conducted. Investigative procedures for workplace accidents and hazardous substance exposures should include:

(a) A visit to the accident scene as soon as possible.

(b) An interview of the injured member and witnesses.

(c) An examination of the workplace for factors associated with the accident/exposure.

(d) Determination of the cause of the accident/exposure.

(e) Corrective action to prevent the accident/exposure from reoccurring.

(f) Documentation of the findings and corrective actions taken.

Additionally the supervisor should proceed with the steps to report an on-duty injury, as required under the Work-Related Disease, Injury and Death Reporting Policy, in conjunction with this investigation to avoid duplication and ensure timely reporting.

1029.9 TRAINING

The Administration Division Supervisor should work with the Training Supervisor to provide all members, including supervisors, with training on general and job-specific workplace safety and health practices. Training shall be provided:

(a) To supervisors to familiarize them with the safety and health hazards to which members under their immediate direction and control may be exposed.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(b) To all members with respect to hazards specific to each member's job assignment.

(c) To all members given new job assignments for which training has not previously been provided.

(d) Whenever new substances, processes, procedures or equipment are introduced to the workplace and represent a new hazard.

(e) Whenever the Department is made aware of a new or previously unrecognized hazard.

1029.9.1 TRAINING TOPICS

The Training Supervisor shall ensure that training includes:

(a) Reporting unsafe conditions, work practices and injuries, and informing a supervisor when additional instruction is needed.

(b) Use of appropriate clothing, including gloves and footwear.

(c) Use of respiratory equipment.

(d) Availability of toilet, hand-washing and drinking-water facilities.

(e) Provisions for medical services and first aid.

(f) Handling of blood borne pathogens and other biological hazards.

(g) Prevention of heat and cold stress.

(h) Identification and handling of hazardous materials, including chemical hazards to which members could be exposed, and review of resources for identifying and mitigating hazards (e.g., hazard labels, Safety Data Sheets (SDS)).

(i) Mitigation of physical hazards, such as heat and cold stress, noise, and ionizing and non-ionizing radiation.

(j) Identification and mitigation of ergonomic hazards, including working on ladders or in a stooped posture for prolonged periods.

(k) Back exercises/stretches and proper lifting techniques.

(l) Avoidance of slips and falls.

(m) Good housekeeping and fire prevention.

(n) Other job-specific safety concerns.

1029.10 RECORDS

Records and training documentation relating to illness and injury prevention will be maintained in accordance with the established records retention schedule.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Line-of-Duty Deaths

1030.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance to members of the Madison County Sheriff's Office in the event of the death of a member occurring in the line of duty and to direct the Department in providing proper support for the member’s survivors.

The Sheriff may also apply some or all of this policy in situations where members are injured in the line of duty and the injuries are life-threatening.

1030.1.1 DEFINITIONS

Definitions related to this policy include:

Line-of-duty death - The death of a sworn member during the course of performing law enforcement-related functions while on- or off-duty, or a non-sworn member during the course of performing their assigned duties.

Survivors - Immediate family members of the deceased member, which can include spouse, children, parents, other next of kin or significant others. The determination of who should be considered a survivor for purposes of this policy should be made on a case-by-case basis given the individual’s relationship with the member and whether the individual was previously designated by the deceased member.

1030.2 POLICY

It is the policy of the Madison County Sheriff's Office to make appropriate notifications and to provide assistance and support to survivors and coworkers of a member who dies in the line of duty.

It is also the policy of this department to respect the requests of the survivors when they conflict with these guidelines, as appropriate.

1030.3 INITIAL ACTIONS BY COMMAND STAFF

(a) Upon learning of a line-of-duty death, the deceased member's supervisor should provide all reasonably available information to the Shift Supervisor and the Dispatch Center.

    (a) Communication of information concerning the member and the incident should be restricted to secure networks to avoid interception by the media or others (see the Public Information Officer section of this policy).

(b) The Shift Supervisor should ensure that notifications are made in accordance with the Officer-Involved Shootings and Deaths and Major Incident Notification policies as applicable.

(c) If the member has been transported to the hospital, the Shift Supervisor or the authorized designee should respond to the hospital to assume temporary responsibilities as the Hospital Liaison.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) The Sheriff or the authorized designee should assign members to handle survivor notifications and assign members to the roles of Hospital Liaison (to relieve the temporary Hospital Liaison) and the Department Liaison as soon as practicable (see the Notifying Survivors section and the Department Liaison and Hospital Liaison subsections in this policy).

1030.4 NOTIFYING SUPERVISORS

Survivors should be notified as soon as possible in order to avoid the survivors hearing about the incident in other ways.

The Sheriff or the authorized designee should review the deceased member's emergency contact information and make accommodations to respect the member's wishes and instructions specific to notifying survivors. However, notification should not be excessively delayed because of attempts to assemble a notification team in accordance with the member's wishes.

The Sheriff, Shift Supervisor or the authorized designee should select at least two members to conduct notification of survivors, one of which may be the Department Chaplain.

Notifying members should:

(a) Make notifications in a direct and compassionate manner, communicating as many facts of the incident as possible, including the current location of the member. Information that is not verified should not be provided until an investigation has been completed.

(b) Determine the method of notifying surviving children by consulting with other survivors and taking into account factors such as the child's age, maturity and current location (e.g., small children at home, children in school).

(c) Plan for concerns such as known health concerns of survivors or language barriers.

(d) Offer to transport survivors to the hospital, if appropriate. Survivors should be transported in department vehicles. Notifying members shall inform the Hospital Liaison over a secure network that the survivors are on their way to the hospital and should remain at the hospital while the survivors are present.

(e) When survivors are not at their residences or known places of employment, actively seek information and follow leads from neighbors, other law enforcement, postal authorities and other sources of information in order to accomplish notification in as timely a fashion as possible. Notifying members shall not disclose the reason for their contact other than a family emergency.

(f) If making notification at a survivor's workplace, ask a workplace supervisor for the use of a quiet, private room to meet with the survivor. Members shall not inform the workplace supervisor of the purpose of their visit other than to indicate that it is a family emergency.

(g) Offer to call other survivors, friends or clergy to support the survivors and to avoid leaving survivors alone after notification.

(h) Assist the survivors with meeting childcare or other immediate needs.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(i) Provide other assistance to survivors and take reasonable measures to accommodate their needs, wishes and desires. Care should be taken not to make promises or commitments to survivors that cannot be met.

(j) Inform the survivors of the name and phone number of the Survivor Support Liaison (see the Survivor Support Liaison section of this policy), if known, and the Department Liaison.

(k) Provide their contact information to the survivors before departing.

(l) Document the survivor’s names and contact information, as well as the time and location of notification. This information should be forwarded to the Department Liaison.

(m) Inform the Sheriff or the authorized designee once survivor notifications have been made so that other Madison County Sheriff's Office members may be apprised that survivor notifications are complete.

1030.4.1 OUT-OF-AREA NOTIFICATIONS

The Department Liaison should request assistance from law enforcement agencies in appropriate jurisdictions for in-person notification to survivors who are out of the area.

- The Department Liaison should contact the appropriate jurisdiction using a secure network and provide the assisting agency with the name and telephone number of the department member that the survivors can call for more information following the notification by the assisting agency.
- The Department Liaison may assist in making transportation arrangements for the member’s survivors, but will not obligate the Department to pay travel expenses without the authorization of the Sheriff.

1030.5 NOTIFYING DEPARTMENT MEMBERS

Supervisors or members designated by the Sheriff are responsible for notifying department members of the line-of-duty death as soon as possible after the survivor notification is made. Notifications and related information should be communicated in person or using secure networks and should not be transmitted over the radio.

Notifications should be made in person and as promptly as possible to all members on-duty at the time of the incident. Members reporting for subsequent shifts within a short amount of time should be notified in person at the beginning of their shift. Members reporting for duty from their residence should be instructed to contact their supervisor as soon as practicable. Those members who are working later shifts or are on days off should be notified by phone as soon as practicable.

Members having a close bond with the deceased member should be notified of the incident in person. Supervisors should consider assistance (e.g., peer support, modifying work schedules, approving sick leave) for members who are especially affected by the incident.

Supervisors should direct members not to disclose any information outside the Department regarding the deceased member or the incident.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

1030.6 PUBLIC INFORMATION OFFICER

In the event of a line-of-duty death, the department's PIO should be the department's contact point for the media. As such, the PIO should coordinate with the Department Liaison to:

(a) Collect and maintain the most current incident information and determine what information should be released.

(b) Ensure that department members are instructed to direct any media inquiries to the PIO.

(c) Prepare necessary press releases.

1. Ensure coordination with other entities having media roles (e.g., outside agencies involved in the investigation or incident).

2. Ensure that important public information is disseminated, such as information on how the public can show support for the department and deceased member's survivors.

(d) Arrange for community and media briefings by the Sheriff or the authorized designee as appropriate.

(e) Respond, or coordinate the response, to media inquiries.

(f) If requested, assist the member's survivors with media inquiries.

1. Brief the survivors on handling sensitive issues such as the types of questions that reasonably could jeopardize future legal proceedings.

(g) Release information regarding memorial services and funeral arrangements to department members, other agencies and the media as appropriate.

(h) If desired by the survivors, arrange for the recording of memorial and funeral services via photos and/or video.

The identity of deceased members should be withheld until the member's survivors have been notified. If the media has obtained identifying information for the deceased member prior to survivor notification, the PIO should request that the media withhold the information from release until proper notification can be made to survivors. The PIO should ensure that media are notified when survivor notifications have been made.

1030.7 DEPARTMENT CHAPLAIN

The Department chaplain may serve a significant role in line-of-duty deaths. His/her duties may include, but are not limited to:

- Assisting with survivor notifications and assisting the survivors with counseling, emotional support or other matters, as appropriate.
- Assisting liaisons and coordinators with their assignments, as appropriate.
- Assisting department members with counseling or emotional support, as requested and appropriate.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Further information on the potential roles and responsibilities of the chaplain are in the Chaplains Policy.

1030.8 INVESTIGATION OF THE INCIDENT

The Sheriff shall ensure that line-of-duty deaths are investigated thoroughly and may choose to use the investigation process outlined in the Officer-Involved Shootings and Deaths Policy.

Investigators from other agencies may be assigned to work on any criminal investigation related to line-of-duty deaths. Partners, close friends or personnel who worked closely with the deceased member should not have any investigative responsibilities because such relationships may impair the objectivity required for an impartial investigation of the incident.

Involved department members should be kept informed of the progress of the investigations and provide investigators with any information that may be pertinent to the investigations.

1030.9 LINE-OF-DUTY DEATH OF A LAW ENFORCEMENT ANIMAL

The Sheriff may authorize appropriate memorial and funeral services for law enforcement animals killed in the line of duty.

1030.10 NON-LINE-OF-DUTY DEATH

The Sheriff may authorize certain support services for the death of a member not occurring in the line of duty.

1030.11 TRAINING

The Training Supervisor should ensure that members are provided training on line-of-duty death benefits within 30 days of employment and every two years thereafter (Va. Code § 9.1-407).

1030.12 LIAISONS AND COORDINATORS

The Sheriff or the authorized designee should select members to serve as liaisons and coordinators to handle responsibilities related to a line-of-duty death, including, but not limited to:

(a) Department Liaison.

(b) Hospital Liaison.

(c) Survivor Support Liaison.

(d) Wellness Support Liaison.

(e) Funeral Liaison.

(f) Mutual aid coordinator.

(g) Benefits Liaison.

(h) Finance coordinator.

Liaisons and coordinators will be directed by the Department Liaison and should be given sufficient duty time to complete their assignments. Members may be assigned responsibilities of more than one liaison or coordinator position depending on available department resources. The Department

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Liaison may assign separate liaisons and coordinators to accommodate multiple family units, if needed.

1030.12.1 DEPARTMENT LIAISON

The Department Liaison should be a Division Supervisor or of sufficient rank to effectively coordinate department resources, and should serve as a facilitator between the deceased member's survivors and the Department. The Department Liaison reports directly to the Sheriff. The Department Liaison's responsibilities include, but are not limited to:

(a) Directing the other liaisons and coordinators in fulfilling survivors' needs and requests. Consideration should be given to organizing the effort using the National Incident Management System (NIMS).

(b) Establishing contact with survivors within 24 hours of the incident and providing them contact information.

(c) Advising survivors of the other liaison and coordinator positions and their roles and responsibilities.

(d) Identifying locations that will accommodate a law enforcement funeral and presenting the options to the appropriate survivors, who will select the location.

(e) Coordinating all official law enforcement notifications and arrangements.

(f) Making necessary contacts for authorization to display flags at half-mast.

(g) Ensuring that department members are reminded of appropriate information-sharing restrictions regarding the release of information that could undermine future legal proceedings.

(h) Coordinating security checks of the member's residence as necessary and reasonable.

(i) Serving as a liaison with visiting law enforcement agencies during memorial and funeral services.

1030.12.2 HOSPITAL LIAISON

The Hospital Liaison should work with hospital personnel to:

(a) Arrange for appropriate and separate waiting areas for:

1. The survivors and others whose presence is requested by the survivors.
2. Department members and friends of the deceased member.
3. Media personnel.

(b) Ensure, as much as practicable, that any suspects who are in the hospital and their families or friends are not in close proximity to the member's survivors or Madison County Sheriff's Office members (except for members who may be guarding the suspect).

(c) Ensure that survivors receive timely updates regarding the member before information is released to others.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Arrange for survivors to have private time with the member, if requested.

1. The Hospital Liaison or hospital personnel may need to explain the condition of the member to the survivors to prepare them accordingly.

2. The Hospital Liaison should accompany the survivors into the room, if requested.

(e) Stay with survivors and ensure that they are provided with other assistance as needed at the hospital.

(f) If applicable, explain to the survivors why an autopsy may be needed.

(g) Ensure hospital bills are directed to the Department, that the survivors are not asked to sign as guarantor of payment for any hospital treatment and that the member's residence address, insurance information and next of kin are not included on hospital paperwork.

Other responsibilities of the Hospital Liaison include, but are not limited to:

- Arranging transportation for the survivors back to their residence.
- Working with investigators to gather and preserve the deceased member's equipment and other items that may be of evidentiary value.
- Documenting his/her actions at the conclusion of his/her duties.

1030.12.3 SURVIVOR SUPPORT LIAISON

The Survivor Support Liaison should work with the Department Liaison to fulfill the immediate needs and requests of the survivors of any member who has died in the line of duty, and serve as the long-term department contact for survivors. The Survivor Support Liaison should be selected by the deceased member's Division Supervisor. The following should be considered when selecting the Survivor Support Liaison:

- The liaison should be an individual the survivors know and with whom they are comfortable working.
- If the survivors have no preference, the selection may be made from names recommended by the deceased member's supervisor and/or coworkers. The deceased member's partner or close friends may not be the best selections for this assignment because the emotional connection to the member or survivors may impair their ability to conduct adequate liaison duties.
- The liaison must be willing to assume the assignment with an understanding of the emotional and time demands involved.

The responsibilities of the Survivor Support Liaison include but are not limited to:

(a) Arranging for transportation of survivors to hospitals, places of worship, funeral homes, and other locations, as appropriate.

(b) Communicating with the Department Liaison regarding appropriate security measures for the family residence, as needed.

(c) If requested by the survivors, providing assistance with instituting methods of screening telephone calls made to their residence after the incident.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Providing assistance with travel and lodging arrangements for out-of-town survivors.

(e) Returning the deceased member's personal effects from the Department and the hospital to the survivors. The following should be considered when returning the personal effects:

1. Items should not be delivered to the survivors until they are ready to receive the items.
2. Items not retained as evidence should be delivered in a clean, unmarked box.
3. All clothing not retained as evidence should be cleaned and made presentable (e.g., items should be free of blood or other signs of the incident).
4. The return of some personal effects may be delayed due to ongoing investigations.

(f) Assisting with the return of department-issued equipment that may be at the deceased member's residence.

1. Unless there are safety concerns, the return of the equipment should take place after the funeral at a time and in a manner considerate of the survivors' wishes.

(g) Working with the Wellness Support Liaison to ensure that survivors have access to available counseling services.

(h) Coordinating with the department's Public Information Officer (PIO) to brief the survivors on pending press releases related to the incident and to assist the survivors with media relations in accordance with their wishes (see the Public Information Officer section of this policy).

(i) Briefing survivors on investigative processes related to the line-of-duty death, such as criminal, internal, and administrative investigations.

(j) Informing survivors of any related criminal proceedings and accompanying them to such proceedings.

(k) Introducing survivors to prosecutors, victim's assistance personnel, and other involved personnel as appropriate.

(l) Maintaining long-term contact with survivors and taking measures to sustain a supportive relationship (e.g., follow-up visits, phone calls, cards on special occasions, special support during holidays).

(m) Inviting survivors to department activities, memorial services, or other functions as appropriate.

Survivor Support Liaisons providing services after an incident resulting in multiple members being killed should coordinate with and support each other through conference calls or meetings as necessary.

The Department recognizes that the duties of a Survivor Support Liaison will often affect regular assignments over many years, and is committed to supporting members in the assignment.

If needed, the Survivor Support Liaison should be issued a personal communication device (PCD) owned by the Department to facilitate communications necessary to the assignment. The

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

department-issued PCD shall be used in accordance with the Personal Communication Devices Policy.

1030.12.4 WELLNESS SUPPORT LIAISON

The Wellness Support Liaison should work with the department wellness coordinator or the authorized designee and other liaisons and coordinators to make wellness support and counseling services available to members and survivors who are impacted by a line-of-duty death. The responsibilities of the Wellness Support Liaison include but are not limited to:

(a) Identifying members who are likely to be significantly affected by the incident and may have an increased need for wellness support and counseling services, including:

1. Members involved in the incident.
2. Members who witnessed the incident.
3. Members who worked closely with the deceased member but were not involved in the incident.

(b) Ensuring that members who were involved in or witnessed the incident are relieved of department responsibilities until they can receive wellness support.

(c) Ensuring that wellness support and counseling resources (e.g., peer support, Critical Incident Stress Debriefing) are available to members as soon as reasonably practicable following the line-of-duty death.

(d) Coordinating with the Survivor Support Liaison to ensure survivors are aware of available wellness support and counseling services and assisting with arrangements as needed.

(e) Following up with members and the Survivor Support Liaison in the months following the incident to determine if additional wellness support or counseling services are needed.

1030.12.5 FUNERAL HOME LIAISON

The Funeral Liaison should work with the Department Liaison, Survivor Support Liaison and survivors to coordinate funeral arrangements to the extent the survivors wish. The Funeral Liaison’s responsibilities include, but are not limited to:

(a) Assisting survivors in working with the funeral director regarding funeral arrangements and briefing them on law enforcement funeral procedures.

(b) Completing funeral notification to other law enforcement agencies.

(c) Coordinating the funeral activities of the Department, including, but not limited to the following:

1. Honor Guard
    (a) Casket watch
    (b) Color guard
    (c) Pallbearers

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Bell/rifle salute

2. Bagpipers/bugler
3. Uniform for burial
4. Flag presentation
5. Last radio call

(d) Briefing the Sheriff and command staff concerning funeral arrangements.

(e) Assigning a deputy to remain at the family home during the viewing and funeral.

(f) Arranging for transportation of the survivors to and from the funeral home and interment site using department vehicles and drivers.

1030.12.6 MUTUAL AID COORDINATOR

The mutual aid coordinator should work with the Department Liaison and the Funeral Liaison to request and coordinate any assistance from outside law enforcement agencies needed for, but not limited to:

(a) Traffic control during the deceased member’s funeral.

(b) Area coverage so that as many Madison County Sheriff's Office members can attend funeral services as possible.

The mutual aid coordinator should perform his/her duties in accordance with the Outside Agency Assistance Policy.

1030.12.7 BENEFITS LIAISON

The Benefits Liaison should provide survivors with information concerning available benefits and will assist them in applying for benefits. Responsibilities of the Benefits Liaison include, but are not limited to:

(a) Confirming the filing of workers’ compensation claims and related paperwork (see the Work-Related Disease, Injury and Death Reporting Policy).

(b) Researching and assisting survivors with application for federal government survivor benefits, such as those offered through the:

1. Public Safety Officers’ Educational Assistance (PSOEA) Program.
2. Social Security Administration.
3. Department of Veterans Affairs.

(c) Researching and assisting survivors with application for state and local government survivor benefits.

1. Surviving spouse and children benefit (Va. Code § 51.1-815).
2. Virginia Line of Duty Act (Va. Code § 9.1-400 et seq.). Information about the benefits available under this Act should be provided to the survivors within 10 days.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

(d) Researching and assisting survivors with application for other survivor benefits such as:

1. Private foundation survivor benefits programs.
2. Survivor scholarship programs.

(e) Researching and informing survivors of support programs sponsored by sheriff's associations and other organizations.

(f) Documenting and informing survivors of inquiries and interest regarding public donations to the survivors.

1. If requested, working with the finance coordinator to assist survivors with establishing a process for the receipt of public donations.

(g) Providing survivors with a summary of the nature and amount of benefits applied for, including the name of a contact person at each benefit office. Printed copies of the summary and benefit application documentation should be provided to affected survivors.

(h) Maintaining contact with the survivors and assisting with subsequent benefit questions and processes as needed.

1030.12.8 FINANCE COORDINATOR

The finance coordinator should work with the Sheriff and the Department Liaison to manage financial matters related to the line-of-duty death. The finance coordinator's responsibilities include, but are not limited to:

(a) Establishing methods for purchasing and monitoring costs related to the incident.

(b) Providing information on finance-related issues, such as:

(a) Paying survivors' travel costs if authorized.

(b) Transportation costs for the deceased.

(c) Funeral and memorial costs.

(d) Related funding or accounting questions and issues.

(c) Working with the Benefits Liaison to establish a process for the receipt of public donations to the deceased member's survivors.

(d) Providing accounting and cost information as needed.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Wellness Program

1031.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance on establishing and maintaining a proactive wellness program for department members.

The wellness program is intended to be a holistic approach to a member's well-being and encompasses aspects such as physical fitness, mental health, and overall wellness.

Additional information on member wellness is provided in the:

- Chaplains Policy.
- Line-of-Duty Deaths Policy.
- Drug- and Alcohol-Free Workplace Policy.

1031.1.1 DEFINITIONS

Definitions related to this policy include:

Critical incident – An event or situation that may cause a strong emotional, cognitive, or physical reaction that has the potential to interfere with daily life.

Critical Incident Stress Debriefing (CISD) – A standardized approach using a discussion format to provide education, support, and emotional release opportunities for members involved in work-related critical incidents.

Peer support – Mental and emotional wellness support provided by peers trained to help members cope with critical incidents and certain personal or professional problems.

1031.2 POLICY

It is the policy of the Madison County Sheriff's Office to prioritize member wellness to foster fitness for duty and support a healthy quality of life for department members. The Department will maintain a wellness program that supports its members with proactive wellness resources, critical incident response, and follow-up support.

1031.3 WELLNESS COORDINATOR

The Sheriff should appoint a trained wellness coordinator. The coordinator should report directly to the Sheriff or the authorized designee and should collaborate with advisers (e.g., Human Resources Department, legal counsel, licensed psychotherapist, qualified health professionals), as appropriate, to fulfill the responsibilities of the position, including but not limited to:

(a) Identifying wellness support providers (e.g., licensed psychotherapists, external peer support providers, physical therapists, dietitians, physical fitness trainers holding accredited certifications).

1. As appropriate, selected providers should be trained and experienced in providing mental wellness support and counseling to public safety personnel.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2. When practicable, the Department should not use the same licensed psychotherapist for both member wellness support and fitness for duty evaluations.

(b) Developing management and operational procedures for department peer support members, such as:

1. Peer support member selection and retention.
2. Training and applicable certification requirements.
3. Deployment.
4. Managing potential conflicts between peer support members and those seeking service.
5. Monitoring and mitigating peer support member emotional fatigue (i.e., compassion fatigue) associated with providing peer support.
6. Using qualified peer support personnel from other public safety agencies or outside organizations for department peer support, as appropriate.

(c) Verifying members have reasonable access to peer support or licensed psychotherapist support.

(d) Establishing procedures for CISDs, including:

1. Defining the types of incidents that may initiate debriefings.
2. Steps for organizing debriefings.

(e) Facilitating the delivery of wellness information, training, and support through various methods appropriate for the situation (e.g., phone hotlines and electronic applications).

(f) Verifying a confidential, appropriate, and timely Employee Assistance Program (EAP) is available for members. This also includes:

1. Obtaining a written description of the program services.
2. Providing for the methods to obtain program services.
3. Providing referrals to the EAP for appropriate diagnosis, treatment, and follow-up resources.
4. Obtaining written procedures and guidelines for referrals to, or mandatory participation in, the program.
5. Obtaining training for supervisors in their role and responsibilities, and identification of member behaviors that would indicate the existence of member concerns, problems, or issues that could impact member job performance.

1031.4 DEPARTMENT PEER SUPPORT

1031.4.1 PEER SUPPORT MEMBER SELECTION CRITERIA

The selection of a department peer support member will be at the discretion of the coordinator. Selection should be based on the member's:

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

- Desire to be a peer support member.
- Experience or tenure.
- Demonstrated ability as a positive role model.
- Ability to communicate and interact effectively.
- Evaluation by supervisors and any current peer support members.

1031.4.2 PEER SUPPORT MEMBER RESPONSIBILITIES
The responsibilities of department peer support members include:

(a) Providing pre- and post-critical incident support.

(b) Presenting department members with periodic training on wellness topics, including but not limited to:

1. Stress management.
2. Suicide prevention.
3. How to access support resources.

(c) Providing referrals to licensed psychotherapists and other resources, where appropriate.

1. Referrals should be made to department-designated resources in situations that are beyond the scope of the peer support member's training.

1031.4.3 PEER SUPPORT MEMBER TRAINING
A department peer support member should complete department-approved training prior to being assigned.

1031.5 CRITICAL INCIDENT STRESS DEBRIEFINGS

A Critical Incident Stress Debriefing should occur as soon as practicable following a critical incident. The coordinator is responsible for organizing the debriefing. Notes and recorded statements shall not be taken because the sole purpose of the debriefing is to help mitigate the stress-related effects of a critical incident.

The debriefing is not part of any investigative process. Care should be taken not to release or repeat any communication made during a debriefing unless otherwise authorized by policy, law, or a valid court order (Va. Code § 19.2-271.4).

Attendance at the debriefing should only include peer support members and those directly involved in the incident.

1031.6 PEER SUPPORT COMMUNICATIONS

Although the Department will honor the sensitivity of communications with peer support members, there is no legal privilege to such communications, except those established by law. Peer support members who are part of a peer support team established under Va. Code § 32.1-111.3 should

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

honor the privilege afforded to communications with covered members related to critical incidents except as permitted or required by law (Va. Code § 19.2-271.4).

1031.7 PHYSICAL WELLNESS PROGRAM

The coordinator is responsible for establishing guidelines for any on-duty physical wellness program, including the following:

(a) Voluntary participation by members

(b) Allowable physical fitness activities

(c) Permitted times and locations for physical fitness activities

(d) Acceptable use of department-provided physical fitness facilities and equipment

(e) Individual health screening and fitness assessment

(f) Individual education (e.g., nutrition, sleep habits, proper exercise, injury prevention) and goal-setting

(g) Standards for fitness incentive programs. The coordinator should collaborate with the appropriate entities (e.g., human resources, legal counsel) to verify that any standards are nondiscriminatory.

(h) Maintenance of physical wellness logs (e.g., attendance, goals, standards, progress)

(i) Ongoing support and evaluation

1031.8 WELLNESS PROGRAM AUDIT

At least annually, the coordinator or the authorized designee should audit the effectiveness of the department's wellness program and prepare a report summarizing the findings. The report shall not contain the names of members participating in the wellness program, and should include the following information:

- Data on the types of support services provided
- Wait times for support services
- Participant feedback, if available
- Program improvement recommendations
- Policy revision recommendations

The coordinator should present the completed audit to the Sheriff for review and consideration of updates to improve program effectiveness.

1031.9 OTHER STATE REQUIREMENTS

The coordinator should make peer support available for deputies whether or not there is a specific incident and should also refer deputies seeking services for mental health to an appropriate mental health professional, as required by Va. Code § 65.2-107.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Wellness Program

1031.10 TRAINING

The coordinator or the authorized designee should collaborate with the Training Supervisor to provide all members with regular education and training on topics related to member wellness, including but not limited to:

- The availability and range of department wellness support systems.
- Suicide prevention.
- Recognizing and managing mental distress, emotional fatigue, post-traumatic stress, and other possible reactions to trauma.
- Alcohol and substance disorder awareness.
- Countering sleep deprivation and physical fatigue.
- Anger management.
- Marriage and family wellness.
- Benefits of exercise and proper nutrition.
- Effective time and personal financial management skills.

Training materials, curriculum, and attendance records should be forwarded to the Training Supervisor as appropriate for inclusion in training records.

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Attachments

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

605 IACP Brady-Giglio Training Outline.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

BRADY/GIGLIO AND OFFICER INTEGRITY

Presented by

Bill Amato

Captain Aaron Jones

Training Objectives

- Acquaint participants with *Brady/Giglio and their application to peace officer integrity*
- Provide perspectives as the issues that surround *Brady/Giglio*
- Identify issues that may present themselves in the future
- Give guidance/examples to developing *Brady/Giglio disclosure procedures for LE agencies*

What the heck is "Brady"?

- Brady v Maryland, 373 U.S. 83 (1963)
- United States v. Giglio, 405 U.S. 150 (1972)
- U.S. v. Bagley, 473 U.S. 667 (1985)
- Kyles v. Whitley, 514 U.S. 419 (1995)
- Strickler v. Green, 527 U.S. 263 (1999)

Brady v. Maryland

- 1963 Capital Murder case
- Government had a duty to disclose material exculpatory evidence
- Failure to do so violated due process –where the evidence is material to either guilty, innocence of the accused or punishment
- There is no regard for good or bad faith of the prosecutor

Brady v. Maryland, USSCt 1963

Under the Constitution, due process requires the prosecution to turn over evidence favorable to the accused and material to his guilt or punishment.

This requirement includes evidence that may be used to impeach the prosecution's witnesses, including police officers.

Brady v. Maryland, USSCt 1963

Police officers and police agencies are, for purposes of

Brady, considered to be part of the prosecution team.

They must therefore make the prosecutor aware of

any evidence that may be favorable to the accused.

United States v. Giglio

- Brady rule includes evidence that could be used to impeach a witness
- When the reliability of a given witness may be determinative of guilt or innocence, non-disclosure of evidence affecting credibility falls within the rule regardless of whether withheld in good faith

U.S. v. Bagley

- No legal distinction between exculpatory evidence and impeachment evidence for purposes of Brady rule
- Favorable evidence is material if there is a reasonable probability that the result would have been different if defense had known
- "harmless error" standard does not apply – issue is whether evidence is material

Kyles v. Whitley

- Knowledge imputed to the prosecution includes knowledge that the police may have
- Prosecutor has a duty to learn of any favorable evidence known to others acting on behalf of the government….this includes the police

Impeachment and Exculpatory Evidence

Examples:

- Government's obligation to disclose favorable evidence under Brady covers not only material exculpatory evidence but also information that could impeach government witnesses
- Agreements exchanging testimony for money or favorable treatment
- The fact the witness suffers from hallucinations
- Efforts by one witness to improperly influence the testimony of other witnesses
- History of untruthfulness
- Other conflicting statements made by witnesses

Material Exculpatory Evidence

Examples:

- Prior inconsistent statements of key witnesses
- Government witnesses had previously filed a false report
- Information undermining the credibility of witness identification of defendant
- Doctor's report following an autopsy which conflicts with later trial testimony

Brady Rule Examples – Exculpatory Evidence

Detective Jones is handling a rape investigation and develops information of a potential suspect who was seen leaving the scene in a white pick-up truck. The investigator displays a photo line-up to the victim and she identifies the suspect, who does own a white pick-up. No forensic evidence connecting the suspect to the crime is initially discovered.

Brady Rule Examples – Exculpatory Evidence

During the course of the investigation, a witness is located during the area canvass who claims to have seen a beige pick-up truck in the area driven by a dark skinned male in his 30's. The identified suspect is a light skinned male in his 20's. The investigator does not document this information in his report because it contradicts the probable cause he has developed in his case.

Brady Rule Examples – Exculpatory Evidence

Detective Smith is handling a murder investigation. He develops a suspect who is of limited intelligence and brings him to the station for questioning. After questioning him over a period of days, he informs the suspect that if he confesses, he will be allowed to go home. The suspect confesses and is taken into custody and charged with murder. Detective Smith fails to document his promise of allowing the suspect to go home in exchange for confessing, and does not inform the prosecutor.

Brady Rule Examples – Exculpatory Evidence

Detective White is handling a robbery investigation in which a victim is shot. He discovers a footprint near the scene, which he has photographed and lifted. He subsequently arrests a suspect who is wearing a size 9 shoe. The foot print is a size 11 sneaker and Detective White discards the footprint evidence believing it is unrelated to the crime. He fails to document this information.

Brady Rule Examples – Exculpatory Evidence

Detective Evans displays photo line-ups to three witnesses. Two of the witnesses identify a suspect; however, the third witness fails to identify anybody. Detective Evans documents the two positive identifications but does not document that the third witness failed to identify the suspect and Detective Evans never informs the prosecutor.

Brady Rule Examples – Officer Credibility Concerns

- Officer investigated, but no finding of violation
- I/A finding that officer had violated policy not relevant or unrelated to truthfulness
- I/A finding that officer made a false or misleading report or statement
- I/A finding that officer had violated policy touching on relevant trait or trial issue
- I/A finding that officer covered up or attempted to cover up

Strickler v. Green

The three essential components of a Brady claim are:

- Evidence favorable to the defendant because it is exculpatory or impeaching;
- The state willfully or inadvertently suppressed the evidence; and
- Prejudice resulted

Brady and Law Enforcement Organizations and their Employees

- Question – does Brady mean we have to disclose evidence that does not show the defendant to be innocent, but mere casts doubt on the testimony of the prosecuting witness?

- YES!

UNTRUTHFULNESS

The term "untruthfulness" refers to false statements, false reports, or intentionally incomplete statements and reports. The false statements involve all aspects of the job, not just enforcement and criminal investigations. See Dreary v. Gloucester, 9 F.3d 191 (1st Cir. 1993) (Ten-year-old disciplinary finding that an officer falsified overtime records admitted for impeachment purposes); United States v. Williams, 1997 WL 335794 (D.D.C. 1997) (New trial ordered because FBI failed to disclose that an agent who was a witness at trial had, fifteen years earlier, received a letter of reprimand for forging an informant's signature on a receipt and lying about the forgery under oath).

BIAS

Bias includes prior records allegedly showing an officer's bias against an identifiable group, i.e., African-Americans or gays. Bias could also be shown toward a particular person or family, based upon prior conduct or statements.

CRIMES

“Crimes” committed by officers which must be disclosed include any crimes other than motor vehicle misdemeanors, DV, or DUI. Even motor vehicle offenses must be disclosed to the prosecutor when the criminal case involves similar conduct.

Brady and Law Enforcement Organizations and Officers

- The belief that Internal Affairs files are confidential and not subject to closure is mistaken
- The adage that the "defendant is on trial, not the officer, has been substantially eroded
- In certain circumstances, the officer's prior conduct is relevant in the criminal trial because that conduct reflects on the officer's credibility

ARE PENDING INVESTIGATIONS OF AN OFFICER SUBJECT TO DISCLOSURE?

Disclosure will assure the integrity of a criminal conviction. The general rule is that unverified or speculative information is not subject to disclosure. However, the decision to disclose such information is best left to the prosecutor.

Potential Brady Material Affecting Officers

- Misconduct involving moral turpitude, untruthfulness
- Bias
- Moral turpitude
- Integrity
- Misdemeanor convictions involving moral turpitude
- Contrary statements about facts of the case
- Evidence undermining the officer's Expertise
- False reports by the Officer in other cases
- Evidence of drug or alcohol addition *

ULTIMATE USE OF THE INFORMATION

Brady information must be disclosed to the prosecutor. The prosecutor must then decide whether to disclose the information to the defense. It is very possible, however, that the information may not be admissible in court. Only that evidence which the court finds to be relevant for impeachment purposes can be used.

THE BOTTOM LINE

- The Department (Officers) should make sure the prosecutor is aware of any information about the officer that, if revealed, would be favorable to the defense.
- The Department (Officers) must disclose to the prosecutor anything in the officer's background that reflects bias, untruthfulness or criminal activity.

THE BOTTOM LINE

- The responsibility to disclose the information belongs to the prosecutor; let them make the decision. You do not want the agency/officer to be held responsible for the retrial of a case due to non-disclosure to the prosecutor.
- All of this applies to both felony and misdemeanor cases.

Prosecutor's Ultimate Role

Prosecution

- Obtain
- Review
- Disclose
- Argue

Non-traditional Sources of Brady Material

- Early Warning Systems –EWS
- Supervisor notes
- E-mails
- Inter-office communications or memorandums
- Annual employee reviews
- Judicial report

Now you know the law, how does it actually work?

- What is the "Brady List"?
- How does an officer get on the list?
- What does being on the list actually mean?
- Can an officer ever get off of the list?

“Brady List”

A Giglio or Brady list is a list compiled usually by a prosecutor's office or a police department containing the names and details of law enforcement officers who have had sustained incidents of untruthfulness, criminal convictions, candor issues, or some other type of issue placing their credibility into question.

Placement On The List

- Police Department/Agencies must disclose information regarding potential Brady/Giglio material to prosecutors

- Prosecutors will then review the information to determine what actions will be taken next

Placement On The List

- Both the law enforcement agency and the prosecutor's office should maintain the list of disclosures

- Prosecutors will then review the disclosures and make case by case determinations as to how to handle the information

What actual issues trigger a Brady Disclosure to Prosecutors?

- The following is not about exculpatory evidence
- Referring to acts/incidents involving law enforcement officers that could call their credibility into question.
- Not just acts of dishonesty.

Hamilton County, OH Prosecutors Request The Following:

- Any criminal record of any witness, or any criminal case pending against any witness, whom the prosecution anticipates calling.

- Information, known to the Department, that casts doubt on the credibility or accuracy of a witness or evidence.

Hamilton County, OH Prosecutors Request The Following:

- Information, known to the Department, regarding any mental or physical impairment of any governmental witness that would cast doubt on his or her ability to testify accurately and truthfully at trial.

- A finding of misconduct by the Civil Service Commission or a completed internal investigation that reflects on an officer or other member of this Department's truthfulness, bias, or moral turpitude. This includes employees under suspension.

Hamilton County, OH Prosecutors Request The Following:

- Evidence that a proposed witness has a racial, religious, or personal bias against a defendant individually or as a member of a group.

- Other information which may be considered as appropriately disclosable Brady material reflecting upon an officer's truthfulness, honesty, bias or misconduct includes, but is not limited to, the following developed from relevant case law:

Hamilton County, OH Prosecutors Request The Following:

(i) lying to superiors during internal/administrative police investigations;

(ii) falsifying police reports or making misleading reports;

(iii) planting evidence;

(iv) theft of evidence in police custody;

(v) failed polygraphs;

(vi) inappropriate records checks of detainees or witnesses;

(vii) any history of lying in the process of testifying or preparing affidavits under oath

Maricopa County Review Process

- Established a review committee for Brady/ Giglio disclosures
- Placement on the "Brady List" is not automatic after a disclosure from LE
- All LE disclosures (called referrals) are vetted through a committee made up of Criminal Chief Prosecutors and LE Liaison

Maricopa County Review Process

- Officers are placed on the "Brady List" after a preponderance of the evidence finding that the referral is Brady/Giglio material
- Once a finding is made, the officer is sent a letter describing the committee's finding
- Will review future administrative findings to determine if placement on the list is still warranted

Cincinnati PD Policy

- Modeled closely to what the Hamilton County Prosecutors requested
- Went through the Cincinnati Police Department Manual or Rules and Regulations and matched specific rule violations with Brady/Giglio requested information
- Created a SOP whereas specific violations were deemed mandatory disclosures

Cincinnati PD Policy

- Other violations can trigger disclosure, but more investigation is warranted

- A database was created where specific violations automatically required additional tasks to close the investigation.

- Prior to closing, there must be an indication of whether disclosure was made to Prosecutors

Can anyone request the Brady List?

- Jurisdictions treat the information differently
- Some jurisdictions are able to send the information directly to the prosecutors office without any formal request
- Other jurisdictions protect personnel/disciplinary files and are only turned over after specific requests/court motions are filed

Can anyone request the Brady List?

- It is important to know and understand the laws procedures within your particular jurisdiction

- There are other groups that have sought Brady/Giglio material/lists other than the prosecutors office

Media Interest In Brady Lists

FOX19 NOW FOX19NOW.com

CRIME

Have officers patrolling your neighborhood been convicted of crimes, lied on job?



Raw interview with Butler Co. Prosecutor Mike Gmoser on the Brady List

By Jennifer Edwards Baker | October 10, 2019 at 9:56 AM EDT
Updated October 11 at 4:10 AM

CINCINNATI (FOX19) - Have the police who patrol your community lied on the job or been convicted of a crimes?

Do you know?

Do prosecutors?

They're supposed to.

Media Interest In Brady Lists

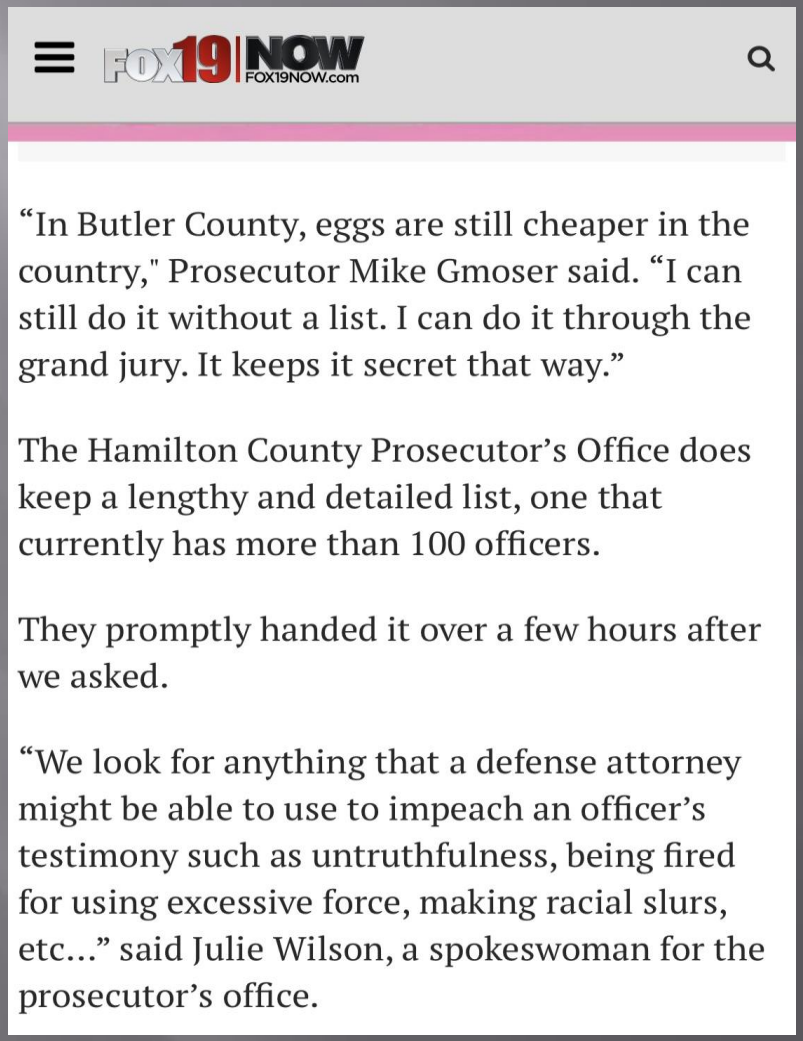
A more than 50-year-old Supreme Court ruling requires prosecutors to seek and disclose evidence to defense attorneys and the accused that is material to his or her guilt or punishment. This includes evidence about their untruthfulness; certain prior criminal convictions and evidence of bias; excessive use of force.

We asked prosecutors across the Tri-State – from Hamilton County to Warren County to Northern Kentucky – to give us their lists, or a copy of their "Brady List."

Most said they do not keep an actual list and some told us they don't have any issues so there simply is no need for one.

One prosecutor is even proud to say he keeps information from the public.

Media Interest In Brady Lists



FOX19NOW FOX19NOW.com

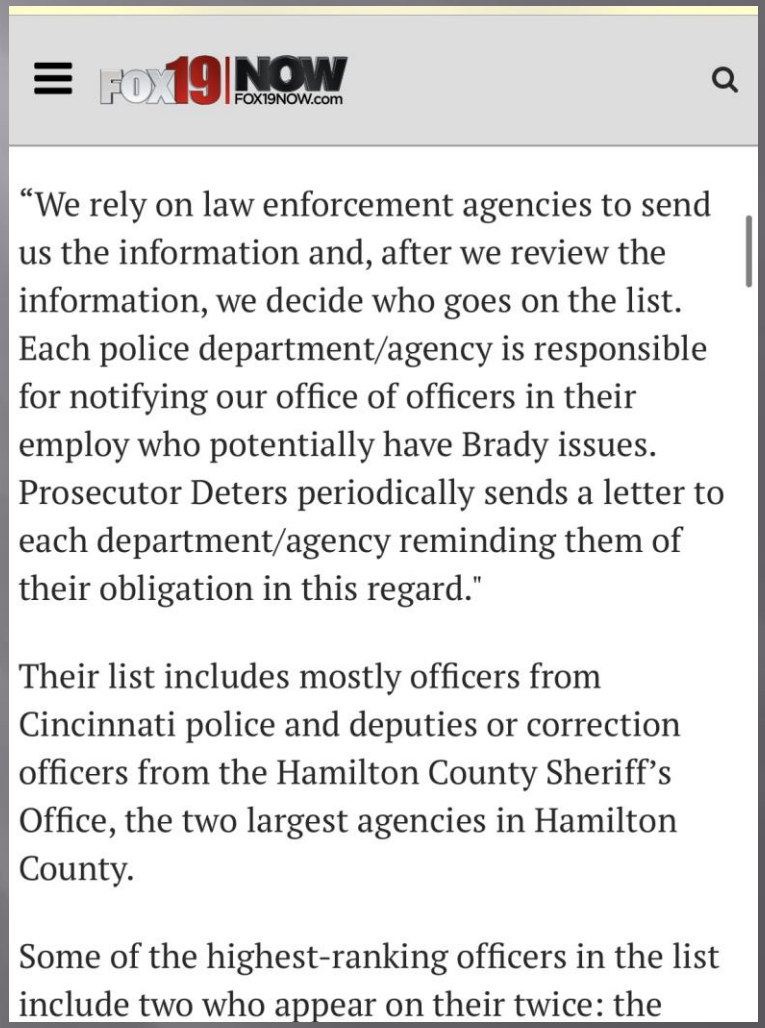
"In Butler County, eggs are still cheaper in the country," Prosecutor Mike Gmoser said. "I can still do it without a list. I can do it through the grand jury. It keeps it secret that way."

The Hamilton County Prosecutor's Office does keep a lengthy and detailed list, one that currently has more than 100 officers.

They promptly handed it over a few hours after we asked.

"We look for anything that a defense attorney might be able to use to impeach an officer's testimony such as untruthfulness, being fired for using excessive force, making racial slurs, etc..." said Julie Wilson, a spokeswoman for the prosecutor's office.

Media Interest in Brady List



FOX19NOW FOX19NOW.com

"We rely on law enforcement agencies to send us the information and, after we review the information, we decide who goes on the list. Each police department/agency is responsible for notifying our office of officers in their employ who potentially have Brady issues. Prosecutor Deters periodically sends a letter to each department/agency reminding them of their obligation in this regard."

Their list includes mostly officers from Cincinnati police and deputies or correction officers from the Hamilton County Sheriff's Office, the two largest agencies in Hamilton County.

Some of the highest-ranking officers in the list include two who appear on their twice: the

Media Interest in Brady Lists

FOX19 NOW
FOX19NOW.com

			Incidents		
14.	[redacted] McCarthy	Colerain Township	Terminated as of April 2015	• Departmental Finding of Dishonesty • Currently in arbitration. If he wins, we still disclose because his own agency made findings of dishonesty.	05/13/2015, **MANDATORY DISCLOSURE** per Phil Cummings.

(**Below names/incidents added to list 7/6/2016 by Phil Cummings/Appellate Division******)**

	Officer's Name & Badge No.	Municipality	Date(s) of Incidents	Findings	Date & Disclosed to Defense
15.	[redacted]	CPD	2/11/15	Plead Guilty to Deer Regulation - Section 1533.11 of OAC[1] - Minor Misdemeanor – Fined $240 – Violation of CPD Rule 1.02 (Criminal Conviction)	**MANDATORY DISCLOSURE:** Criminal Conviction of State's Witness. Prosecutor to Argue Minimal Relevance/Lack of Impeachment Value at Trials
16.	[redacted]	CPD	6/30/2014	Plead No Contest to Attempted Tampering with Evidence – R.C. 2923.02 and Illegal Use of a Minor in Nudity Oriented Material – R.C. 2907.323. Sentence: 1 Year ODC – Violation of CPD Rule 1.02 (Criminal Conviction)	**MANDATORY DISCLOSURE:** Criminal Conviction of State's Witness. Terminated by CPD

Media Interest in Brady List

FOX19NOW FOX19NOW.com

MANDATORY DISCLOSURE OF IMPEACHING EVIDENCE TO PROSECUTORS

Per *Brady and Giglio*, this information must be disclosed to defense counsel in discovery

	Officer's Name & Badge No.	Municipality	Date(s) of Incidents	Findings	Date & Disclosed to Defense
1.	[redacted]	CPD	11/18/2009	IIS of CPD found Kinney used Excessive Force (against Dewayne White) and Kinney also sustained a Rule 5.01 Dishonesty Violation	**DISCLOSURE:** Beginning Feb. 2013. Bill Breyer prepared a brief write up for Prosecutors to use. See doc. #00416319. *Media articles (Fox 19 & Cinti Enquirer) also written about this.
2.	[redacted]	CPD	11/18/2009	Rule 5.01 Dishonesty Violation	**DISCLOSURE** (As of Feb. 2013) See doc #00416319
3.	[redacted]	Springfield Twp. PO	Prior to 3/26/2012	*Internal Investigation Report of Acts of Dishonesty dated 3/26/2012 *Terminated by Springfield Township effective 4/4/2012	**DISCLOSURE:** HCPROS Memo sent 4/12/12 to all criminal prosecutors informing them of violation and officer's termination.
4.	[redacted]	North College Hill Police (formerly)	8/21/2012	P.O. Roos indicted federally in August 2012 for his involvement in Marijuana trafficking conspiracy/money laundering scheme (11 total charged)	**DISCLOSURE:** *HCPROS Memo sent 8/23/2012 to all prosecutors alerting them to possible discovery issues with this officer. *In October 2013 Roos sentenced to probation in federal court (No. 1:12-CR-080-11) to Ct. 14 of indictment, and agreed to resign his position as a police officer and not seek reinstatement.

Brady Websites

- Bradycops.org
- Website attempting to compile a national list of officers placed on Brady lists

Consequences of Placement on the "Brady List"

- Stigma or damage to officer's reputation
- Limit job assignments
- Limit advancement through the agency
- Possibly termination if the officer is no longer credible to give testimony and no other administrative assignment is available in the department

- If you are a Chief or Sheriff, what do you do?

Can An Officer Be Removed From the List?

- An original disclosure that is later determined to be unfounded or not sustained could be a basis to remove the officer from the list
- Some courts have required a removal from the list after an arbitrator has exonerated the officer
- That Depends (the great Lawyer answer)

Trends

- Legislative Intervention
- 13 States have passed legislation specific to "Brady Lists"
  - Check your state and prosecutor
- Legislate
  - Notice
  - Ability to appeal
  - Restorative Justice (ability to get off list)
  - Personnel actions

Questions?

Rappahannock Rapidan Transfer of Custody Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Rappahannock Rapidan CIT Assessment Center
Transfer of Custody Form

NAME OF RESPONDENT _____ DATE OF BIRTH _____ SSN _____ GENDER _____

RESIDENCE ADDRESS _____ CITY _____ STATE _____ ZIP CODE _____

Individual was taken into Emergency Custody Pursuant to:
[] § 37.2-808: Initiated by an order issued by the Office of the Magistrate, which is attached;
This Emergency Custody will expire at _____.
OR
[] § 37.2-808 G: Initiated by a Law Enforcement Officer;
Emergency Custody was executed at _____ based upon observation or reliable reports.
This Emergency Custody will expire at _____.

Name of Law Enforcement Officer _____ Agency and Badge # _____

Signature of Law Enforcement Officer _____ Date and Time CITAC Notified by Law Enforcement _____

For Use by Officer/Deputy: Are you CIT-Trained? ☐ Yes ☐ No **Date & Time Intervention Initiated:** _____

Call Type: ☐ Dispatched, Mental Health ☐ Dispatched, ECO ☐ Dispatched, Wellness Check ☐ Self-Initiated

On-Scene Injuries: ☐ None ☐ Officer/Deputy ☐ Individual ☐ Both

Would criteria have been met for discretionary arrest? ☐ Yes ☐ No What would the charges have been? _____

[] New Horizon Security Officer accepts a Transfer of Custody for this individual pursuant to § 37.2-808 E, and in accordance with the Memorandum of Agreement establishing the policies and procedures for such transfer.
[] New Horizon Security Officer refused to accept Transfer of Custody because: [] Lack capacity; [] referral not appropriate; [] medical issue; or [] Other_____

Name of New Horizon Security Officer _____ Badge # _____ Date and Time of Arrival at CITAC _____

Signature of New Horizon Security Officer _____ Date and Time Custody Transferred to New Horizon Officer _____

[] Individual was transported to _____ for medical assessment at _____ and was [] medically cleared at _____ OR [] medically admitted at _____

[] Individual and the ECO have been released as the Individual was found to not meet TDO criteria at this time. [] Check, if for Medical Reasons
[] Individual and the ECO have been released as the Individual has agreed to be admitted voluntarily.
[] Individual meets TDO Criteria and a TDO will be petitioned once an accepting facility is located.

Name of Certified Prescreener _____ Signature of Certified Prescreener _____ Date and Time _____

New Horizon Security Officer requested law enforcement officers to respond/return to resume/take custody of this individual as [] N/A;
[] A change has occurred and New Horizon Security can no longer provide for the security of the individual or others; OR
[] A TDO has been issued for a non-local accepting facility and law enforcement officers will be required to transport the individual; OR
[] CCSO is unable to conduct the transport and law enforcement officers will be required to transport the individual to the local accepting facility.

Date and Time request made/TDO Issued _____ Date and Time of Transfer to Law Enforcement _____

Name of New Horizon Security Officer – Badge # _____ Name of Law Enforcement Officer – Agency and Badge # _____

Signature of New Horizon Security Officer – Badge # _____ Signature of Law Enforcement Officer – Agency and Badge _____

If CITAC Conducts TDO Transport: Facility transported to _____

Departure Time to Facility_____ Arrival Time at Facility_____ Return Time to CITAC_____

Version 1.0: 1/4/2015

Detainee Personal Property Record Receipt.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Madison County Sheriff's Office
Detainee Personal Property Record/Receipt

Detainee Name:	DOB:
Emergency Contact Name:	Phone #

MEDICAL

1. HOW IS YOUR HEALTH TODAY?_____
2. DO YOU HAVE ANY MEDICAL PROBLEMS?_____
3. DO YOU HAVE ANY CURRENT ILLNESS OR INJURIES?_____
4. ARE YOU PREGNANT?_____
5. ARE YOU CURRENTLY UNDER DOCTORS CARE?_____
6. DO YOU SUFFER FROM SEIZURES, ARE EPILEPTIC OR DIABETIC?_____
7. HAVE YOU HAD ANY RECENT SURGERIES?_____
8. HAVE YOU EVERY ATTEMPTED SUICIDE, THOUGH ABOUT OR ARE THINKING ABOUT HARMING YOURSELF NOW?_____

PERSONAL PROPERTY INVENTORY (LIST BELOW INCLUDE CLOTHING DESCRIPTION)

CASH $	
COINS $	
TOTAL MONEY $	

I certify this is a correct list of the items removed from my possession at the Madison County Sheriff's Office this _____day of _____,20__

_____
DETAINEE SIGNATURE

_____
SIGNATURE OF OFFICER COMPLETING FORM, DATE & TIME

PROPERTY RELEASE: I CERTIFY I HAVE RECEIVED ALL ITEMS LISTED ABOVE:

_____
DETAINEE SIGNATURE

○ Property not released to detainee/Property transported to Jail

_____
SIGNATURE OF OFFICER COMPLETING FORM, DATE & TIME

Madison County Sexual Assault Response Team MOU (10-30-2020).pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

COUNTY OF MADISON, VIRGINIA
SEXUAL ASSAULT RESPONSE TEAM ("SART")

MEMORANDUM OF UNDERSTANDING

October 30, 2020

I. INTRODUCTION

The County of Madison (Va.) Sexual Assault Response Team ("SART"), established pursuant to Section 15.2-1627.4 of the Code of Virginia, consists of local agencies responsible for responding to victims of sexual assault. The purpose of this agreement is to enhance the collaboration of these partner agencies as well as delineate agency responsibilities in responding to reported incidents of sexual assaults.

This memorandum of understanding ("MOU") shall supersede any prior SART agreements or protocols for the County of Madison, and shall remain in effect unless otherwise amended by agreement of all parties, or until any party terminates their commitment in writing.

II. MEMBERSHIP

Membership in the SART shall be comprised of representatives from the following agencies:

1. Commonwealth's Attorney's Office for the County of Madison
2. Madison County Sheriff's Office ("MCSO")
3. Services for Abused Families, Inc. ("SAFE")
4. Madison County Victim/Witness Program ("Victim/Witness")
5. University of Virginia Health System, Forensic Nurse Examiners

All members shall designate a liaison to participate actively on the SART.

III. SART MEMBER RESPONSIBILITIES

The Office of the Commonwealth's Attorney agrees to:

- Convene a meeting, at least annually, to discuss implementation of protocols and policies for the SART;

- Establish guidelines in collaboration with team partners for the community's response, including the collection, preservation, and secure storage of evidence from Physical Evidence Recovery Kits ("PERKs");

- Ensure an annual review of established guidelines;

- Refer sexual assault victims, family members and friends to SAFE for crisis intervention, advocacy, and counseling services, as appropriate;

- Refer sexual assault victims, family members and friends to Victim/Witness for information about victims' rights, assistance with filing for victims' compensation, and support navigating the criminal justice, as appropriate;

- Allow a sexual assault or victim advocate, unless refused by the victim, to be present during interviews conducted by the Commonwealth;

- Promote policies and practice to increase arrest and prosecution rates for criminal sexual assault, including non-stranger sexual assault;

- Use Forensic Nurse Examiners (FNEs) or Sexual Assault Nurse Examiners (SANEs) as witnesses during sexual assault trials, as appropriate;

- Provide reasonable notification of upcoming trials to the health care provider and/or FNE/SANE who will be called to testify;

- Contact the health care provider and/or FNE/SANE prior to testimony to review the case; and

- Participate, as appropriate, in cross training with allied professionals regarding response to sexual assault.

The Madison County Sheriff's Office agrees to:

- Refer all acute adult sexual assault victims to the hospital and/or a FNE/SANE program for medical treatment and/or a forensic exam;

- Inform sexual assault victims that they are not required to make a report or talk to a law enforcement officer in order to have a forensic exam;

- Transport or arrange for transport of sexual assault victims to the hospital and, once the PERK exam is complete, transport or arrange for transport of victims to a safe location;

- Notify the hospital and/or the FNE/SANE program that a sexual assault victim is being transported;

- Request the assistance of a sexual assault advocate, unless refused by the victim, from either SAFE or the Sexual Assault Resource Agency in Charlottesville depending on availability;

- Perform a suspect evidence collection kit or provide kit to FNE/SANE program to perform, as appropriate;

- Receive medical/forensic evidence that has been collected from victims and/or perpetrators;

- Follow MCSO established protocol regarding evidence collection and storage;

- Coordinate interview processes and/or conduct joint interviews with the hospital and/or FNE/SANE, as the case dictates appropriate;

- Allow the sexual assault advocate, unless refused by the victim, to be present during interviews and/or other communications with officers/investigators;

- Promote policies and practice that increase arrest and prosecution rates for criminal sexual assault, including non-stranger sexual assault;

- Support the development and annual review of the community's guidelines; and

- Participate, as appropriate, in cross training with allied professionals regarding response to sexual assault.

Services to Abused Families (SAFE) agrees to:

- Provide trained sexual assault advocates to meet with victims, family members and friends;

- Provide crisis intervention, advocacy, counseling, criminal justice information and support, and court preparation and orientation for sexual assault victims, as appropriate;

- Coordinate the above victim assistance services for victims, family members and friends with the local Victim/Witness Program, as appropriate;

- Refer sexual assault victims to the hospital, as appropriate;

- Support the development and annual review of the community's guidelines; and

- Participate, as appropriate, in cross training with allied professionals regarding response to sexual assault.

The University of Virginia Health System, Forensic Nurse Examiners agree to:

- Promote a reasonable response time from the time the call is received to the time the trained health care provider and/or FNE/SANE arrives at the hospital;

- Conduct medical/forensic examinations for sexual assault patients in accordance with all agreed-upon protocols and procedures;

- Provide private examination rooms and supplies, including PERKs, necessary for the completion of the medical/forensic examinations;

- Assure that a sexual assault advocate has been notified that a victim is being transported or has arrived;

- Encourage/support use of a sexual assault advocate for sexual assault patients as appropriate and regardless of the patient's decision regarding contact with law enforcement;

- Maintain chain of custody of forensic evidence and transfer to a law enforcement agency or officer;

- Work in collaboration with the local law enforcement agency(s) to ensure adequate supply of PERKs;

- Be available to criminal justice professionals to review the case;

- Maintain contact and communication with criminal justice professionals;

- Support the development and annual review of the community's guidelines; and

- Participate, as appropriate, in cross training with allied professionals regarding response to sexual assault.

The Madison County Victim/Witness Program agrees to:

- Provide resource and referral to counseling and area resources;

- Provide crisis intervention, criminal justice information and support, courtroom assistance, and court preparation and orientation, as appropriate;

- Coordinate the above services for victims, family members and friends with SAFE, as appropriate;

- Provide assistance in obtaining family abuse or stalking protective orders;

- Facilitate the provision of separate waiting areas for victims and witnesses of crime;

- Provide assistance in the processing and filing of crime victims' compensation; in obtaining return of the victim's property when used as evidence; in obtaining restitution for economic loss; and in facilitating reimbursement for mileage and lodging for out of town witnesses, as appropriate;

- Upon request of the victim, provide notifications of friends, relatives, and employers of the occurrence of the crime; intervention with employers to prevent loss of pay or other benefits resulting from the crime or participation in the criminal justice system; notices of court dates; and status of release of defendants or prisoners from custody;

- Assist victims in filing a victim impact statement, which affords the survivor the opportunity to tell the court, in writing, the impact of the crime;

- Ensure that victims have reasonable notification of upcoming hearing and/or trial dates;

- Ensure the victim meets with Commonwealth's Attorney, as appropriate, prior to hearings and/or trial;

- Support the development and annual review of the community's guidelines; and

- Participate, as appropriate, in cross training with allied professionals regarding response to sexual assault.

---ENDORSEMENTS ON FOLLOWING PAGE---

IV. ENDORSEMENTS

The following parties agree to adhere to the terms of this Agreement:

Clarissa T. Berry — Oct 30, 2020

Commonwealth's Attorney — Date
Office of the Commonwealth's Attorney

Erik J. Weaver — Jan 25, 2021
Erik J. Weaver (Jan 25, 2021 15:34 EST)

Sheriff — Date
Madison County Sheriff's Office

Cindy Hedges — Nov 4, 2020
Cindy Hedges (Nov 4, 2020 09:19 EST)

Executive Director — Date
Services to Abused Families (SAFE)

Jeanne Parrish, FNP — Jan 25, 2021
Jeanne Parrish, FNP (Jan 25, 2021 13:44 EST)

FNE/SANE Program Coordinator — Date
University of Virginia Health System

Jennifer Hayes — Nov 4, 2020
Jennifer Hayes (Nov 4, 2020 08:58 EST)

Director — Date
Victim/Witness Program

Madison County SART - Final 10.30.2020

Final Audit Report 2021-01-25

Created:	2020-10-30
By:	Wade Gelbert (wgelbert@madisonco.virginia.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAFCH9Q0YmV2SZuBlNbBq__T4U8D0tw2li

"Madison County SART - Final 10.30.2020" History

Document created by Wade Gelbert (wgelbert@madisonco.virginia.gov)
2020-10-30 - 6:08:14 PM GMT- IP address: 70.33.146.110

Document emailed to Clarissa Berry (cberry@madisonco.virginia.gov) for signature
2020-10-30 - 6:16:51 PM GMT

Document e-signed by Clarissa Berry (cberry@madisonco.virginia.gov)
E-signature obtained using URL retrieved through the Adobe Sign API
Signature Date: 2020-10-30 - 6:18:35 PM GMT - Time Source: server- IP address: 70.33.146.110

Document emailed to Jennifer Hayes (jhayes@madisonco.virginia.gov) for signature
2020-10-30 - 6:18:37 PM GMT

Email viewed by Jennifer Hayes (jhayes@madisonco.virginia.gov)
2020-11-04 - 1:56:38 PM GMT- IP address: 70.33.146.110

Document e-signed by Jennifer Hayes (jhayes@madisonco.virginia.gov)
Signature Date: 2020-11-04 - 1:58:39 PM GMT - Time Source: server- IP address: 70.33.146.110

Document emailed to Cindy Hedges (director@safejourneys.org) for signature
2020-11-04 - 1:58:41 PM GMT

Email viewed by Cindy Hedges (director@safejourneys.org)
2020-11-04 - 2:15:56 PM GMT- IP address: 73.147.37.52

Document e-signed by Cindy Hedges (director@safejourneys.org)
Signature Date: 2020-11-04 - 2:19:57 PM GMT - Time Source: server- IP address: 73.147.37.52

Document emailed to Jeanne Parrish, FNP (jrd4e@virginia.edu) for signature
2020-11-04 - 2:19:58 PM GMT

Email viewed by Jeanne Parrish, FNP (jrd4e@virginia.edu)
2020-11-04 - 2:28:51 PM GMT- IP address: 99.203.145.186

Document e-signed by Jeanne Parrish, FNP (jrd4e@virginia.edu)
Signature Date: 2021-01-25 - 6:44:38 PM GMT - Time Source: server- IP address: 137.54.125.246

Document emailed to Erik J. Weaver (mcsheriff@madisonco.virginia.gov) for signature
2021-01-25 - 6:44:40 PM GMT

Email viewed by Erik J. Weaver (mcsheriff@madisonco.virginia.gov)
2021-01-25 - 6:45:34 PM GMT- IP address: 70.33.146.107

Document e-signed by Erik J. Weaver (mcsheriff@madisonco.virginia.gov)
Signature Date: 2021-01-25 - 8:34:12 PM GMT - Time Source: server- IP address: 70.33.146.107

Agreement completed.
2021-01-25 - 8:34:12 PM GMT

Adobe Sign

Ride-Along Application and Liability Waiver.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Madison County Sheriff's Office
RIDE-ALONG
APPLICATION, AND WAIVER FORM

Regulations

No person will be allowed to ride without having submitted a signed Ride-Along Application and Waiver and Release of Claim. False statements of any nature on the form, will disqualify an individual from participation in the program. Applications are accepted on a discretionary basis.

Ride-alongs will report to Madison County Sheriff' Office fifteen minutes prior to the scheduled start time. Ride-alongs should dress in either business attire or neat, clean, casual attire. Jeans, shorts, spandex, leggings, T-shirts and sweats and clothing bearing offensive or controversial logos or messages are not acceptable. Ride-alongs will not be allowed to carry a weapon. The participant will always follow the directions of their assigned officer escort.

Ride-alongs will be allowed to observe as much of any situation as is possible, consistent with their safety; however, they may not leave the police vehicle unless given permission to do so by their officer escort. Ride-alongs are prohibited from entering any private residence without the express consent of the resident or other authorized person.

The ride-along participant is an observer only. Ride-alongs will not become involved in any investigation, handling of evidence, discussions with victims, witnesses, or suspects, reading an individual's criminal history or other protected information, or handling of any department equipment. Officer escorts may not allow Ride-alongs to be present in any location or situation that would jeopardize the Ride-along's safety or cause undue stress or embarrassment to a victim or any other member of the public. Participants may be allowed to continue a ride-along during the transportation and booking process, provided it does not jeopardize their safety.

Cameras and tape recorders are not permitted. Officer escorts may permit their ride-along observer to take one photograph of themselves with their assigned officer escort and his/her assigned vehicle before departing from or upon returning to Madison County Sheriff's Office if they wish. Ride-alongs must pay for their own food and beverages. If possible, they will be given an opportunity to eat a meal; however, this will depend on the level of calls for service.

The officer escort may terminate the ride for just cause, including if the participant fails to follow the regulations or is acting in a manner inconsistent with the best interests of the Madison County Sheriff's Office. The participant may request that the ride be terminated at any time. In such cases, the Ride-along will be returned to the Madison County Sheriff's Office as soon as possible.

WAIVER AND RELEASE OF CLAIM

As a condition precedent to being permitted to participate as a Ride-Along Observer in a vehicle operated by any officer or person employed by Madison County, Virginia I the undersigned, agree to abide by the above regulations, and herby waive any claim I may have against Madison County, Virginia and the elected or appointed officers, agents and employees of Madison County for any loss of life, physical or emotional injury, property damage or any other claim whatsoever that I may have as a result of any and all conditions, injuries or loss of property sustained during or as a result of riding as such Ride-Along Observer. I further agree that this waiver of liability by me is binding on my legal representatives, heirs, and successors, and shall have the same legal effect as I have agreed to herein.

SIGNATURE OF PARTICIPANT: _____ **DATE:** _____

PRINT NAME: _____

SIGNATURE OF PARENT, GUARDIAN, OR WITNESS

(If Ride-along is a minor): _____ **DATE:** _____

Please fill out the Application on the back page.

Madison County Sheriff' Office

Ride-Along Application

NAME_____ DATE OF BIRTH_____ RACE ___ SEX ___ AGE ____
(Please Print)

HOME ADDRESS_____ CITY, STATE, ZIP _____

DRIVERS LICENSE #_____ HOME PHONE # _____

BUSINESS NAME _____ BUSINESS PHONE # _____

IN CASE OF EMERGENCY NOTIFY: _____ PHONE # _____

RIDING TIME DESIRED: *(CHECK ONE)* ☐ DAY SHIFT ☐ EVENING SHIFT ☐ MIDNIGHT SHIFT

REPORTING TIME_____ DAY OF WEEK DESIRED_____ 2ND CHOICE _____

HAVE YOU PARTICIPATED IN A GCPD RIDE-ALONG WITHIN THE LAST 12 MONTHS? YES ☐ NO ☐

WHAT PROMPTED YOUR INTEREST IN THE RIDE-ALONG PROGRAM? _____

Initial acknowledging that you understand a Criminal History will be checked before ride along will be approved_____

(Madison County Sheriff's Office use only)

TO BE COMPLETED BY DIVISION COMMANDER (or designee)

NCIC/GCIC CHECK MADE _____ NO RECORD ☐ RECORD ATTACHED ☐
(Date)

APPLICANT NOTIFIED BY _____ DATE _____

DATE AND TIME SCHEDULE FOR RIDE-ALONG _____

ASSIGNED OFFICER BADGE NO.

_____ _____ _____

APPROVED ☐ DISAPPROVED ☐ TERMINATED ☐

TO BE COMPLETED BY OFFICER ESCORT

WOULD YOU RECOMMEND THE INDIVIDUAL BE ALLOWED TO RETURN FOR ANOTHER RIDE-ALONG?

YES NO EXPLAIN _____

DIVISION COMMANDER SIGNATURE _____ DATE _____

408 Bomb Threat Procedures and Checklist.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

BOMB THREAT PROCEDURES

This quick reference checklist is designed to help employees and decision makers of commercial facilities, schools, etc. respond to a bomb threat in an orderly and controlled manner with the first responders and other stakeholders.

Most bomb threats are received by phone. Bomb threats are serious until proven otherwise. Act quickly, but remain calm and obtain information with the checklist on the reverse of this card.

If a bomb threat is received by phone:

1. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.
2. Listen carefully. Be polite and show interest.
3. Try to keep the caller talking to learn more information.
4. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
5. If your phone has a display, copy the number and/or letters on the window display.
6. Complete the Bomb Threat Checklist immediately. Write down as much detail as you can remember. Try to get exact words.
7. Immediately upon termination of call, DO NOT HANG UP, but from a different phone, contact authorities immediately with information and await instructions.

If a bomb threat is received by handwritten note:

- Call _____
- Handle note as minimally as possible.

If a bomb threat is received by e-mail:

- Call _____
- Do not delete the message.

Signs of a suspicious package:

- No return address
- Excessive postage
- Stains
- Strange odor
- Strange sounds
- Unexpected delivery
- Poorly handwritten
- Misspelled words
- Incorrect titles
- Foreign postage
- Restrictive notes

**** Refer to your local bomb threat emergency response plan for evacuation criteria***

DO NOT:

- Use two-way radios or cellular phone. Radio signals have the potential to detonate a bomb.
- Touch or move a suspicious package.

WHO TO CONTACT (Select One)

- **911**
- **Follow your local guidelines**

For more information about this form contact the DHS Office for Bombing Prevention at OBP@dhs.gov

Homeland Security

2014

BOMB THREAT CHECKLIST

DATE: **TIME:**

TIME CALLER HUNG UP: **PHONE NUMBER WHERE CALL RECEIVED:**

Ask Caller:

- Where is the bomb located? (building, floor, room, etc.)
- When will it go off?
- What does it look like?
- What kind of bomb is it?
- What will make it explode?
- Did you place the bomb? Yes No
- Why?
- What is your name?

Exact Words of Threat:

Information About Caller:

- Where is the caller located? (background/level of noise)
- Estimated age:
- Is voice familiar? If so, who does it sound like?
- Other points:

Caller's Voice

- ☐ **Female**
- ☐ **Male**
- ☐ Accent
- ☐ Angry
- ☐ Calm
- ☐ Clearing throat
- ☐ Coughing
- ☐ Cracking voice
- ☐ Crying
- ☐ Deep
- ☐ Deep breathing
- ☐ Disguised
- ☐ Distinct
- ☐ Excited
- ☐ Laughter
- ☐ Lisp
- ☐ Loud
- ☐ Nasal
- ☐ Normal
- ☐ Ragged
- ☐ Rapid
- ☐ Raspy
- ☐ Slow
- ☐ Slurred
- ☐ Soft
- ☐ Stutter

Background Sounds

- ☐ Animal noises
- ☐ House noises
- ☐ Kitchen noises
- ☐ Street noises
- ☐ Booth
- ☐ PA system
- ☐ Conversation
- ☐ Music
- ☐ Motor
- ☐ Clear
- ☐ Static
- ☐ Office machinery
- ☐ Factory machinery
- ☐ Local
- ☐ Long Distance

Other Information:

Threat Language

- ☐ Incoherent
- ☐ Message read
- ☐ Taped message
- ☐ Irrational
- ☐ Profane
- ☐ Well-spoken

MCSO Instructions for Photo Array.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Instructions for Sequential Photo Array

In a moment, I am going to show you a series of photos. The person who committed the crime may or may not be included. I do not know whether the person being investigated is included. Even if you identify someone during this procedure, I will continue to show you all photos in the series. Keep in mind that things like hairstyles, beards, and mustaches can be easily changed and that complexion colors may look slightly different in photographs.

You should not feel you have to make an identification. This procedure is important to the investigation whether you identify someone. Regardless of whether you identify any suspect as the perpetrator, the police investigation is still ongoing.

The photos will be shown to you one at a time and are not in any order. Take as much time as you need to look at each one. You will be shown all photos. After each photo, I will ask you "Is this the person you saw [Insert Description]?" Take your time answering the question. If you answer "yes" I will ask you, "Are you sure?"

Because you are involved in an ongoing investigation, in order to prevent damaging the investigation, you should avoid discussing this identification procedure or its results.

Do you understand the way the photo array procedure will be conducted and the other instructions I have given?

I have read these instructions and understand the instructions. I am prepared to receive the photographs that will be presented to me, and I will follow the instructions provided on this form.

Date/Time: _____ Location: _____

Officer: _____ Officer Signature: _____

Witness Name: _____ Witness Signature: _____

Instructions for Sequential Photo Array

I have indicated that photo #_____is the person who (describe the act witnessed):

_____

_____

_____

Witness Initials: _____

Witness Affirmation Statement:

_____

_____

_____

Witness Signiture: _____

Officer Signiture: _____

805 CJIS Security Policy Rev. 5.9.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS) Security Policy

Version 5.9
06/01/2020

CJISD-ITS-DOC-08140-5.9

Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

EXECUTIVE SUMMARY

Law enforcement needs timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In response to these needs, the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure in 1998. Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI). The Federal Information Security Management Act of 2002 provides further legal basis for the APB approved management, operational, and technical security requirements mandated to protect CJI and by extension the hardware, software and infrastructure required to enable the services provided by the criminal justice community.

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology. The Policy is presented at both strategic and tactical levels and is periodically updated to reflect the security requirements of evolving business models. The Policy features modular sections enabling more frequent updates to address emerging threats and new security measures. The provided security criteria assists agencies with designing and implementing systems to meet a uniform level of risk and security protection while enabling agencies the latitude to institute more stringent security requirements and controls based on their business model and local needs.

The CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Bureaus (SIB). Further, as use of criminal history record information for noncriminal justice purposes continues to expand, the CJIS Security Policy becomes increasingly important in guiding the National Crime Prevention and Privacy Compact Council and State Compact Officers in the secure exchange of criminal justice records.

The Policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. The Policy empowers CSAs with the insight and ability to tune their security programs according to their risks, needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities.

CHANGE MANAGEMENT

Revision	Change Description	Created/Changed by	Date	Approved By
5	Policy Rewrite	Security Policy Working Group	2/9/2011	See Signature Page
5.1	Incorporate Calendar Year 2011 APB approved changes and administrative changes	CJIS ISO Program Office	7/13/2012	APB & Compact Council
5.2	Incorporate Calendar Year 2012 APB approved changes and administrative changes	CJIS ISO Program Office	8/9/2013	APB & Compact Council
5.3	Incorporate Calendar Year 2013 APB approved changes and administrative changes	CJIS ISO Program Office	8/4/2014	APB & Compact Council
5.4	Incorporate Calendar Year 2014 APB approved changes and administrative changes	CJIS ISO Program Office	10/6/2015	APB & Compact Council
5.5	Incorporate Calendar Year 2015 APB approved changes and administrative changes	CJIS ISO Program Office	6/1/2016	APB & Compact Council
5.6	Incorporate Calendar Year 2016 APB approved changes and administrative changes	CJIS ISO Program Office	6/5/2017	APB & Compact Council
5.7	Incorporate Calendar Year 2017 APB approved changes and administrative changes	CJIS ISO Program Office	08/16/2018	APB & Compact Council
5.8	Incorporate Calendar Year 2018 APB approved changes and administrative changes	CJIS ISO Program Office	06/01/2019	APB & Compact Council
5.9	Incorporate Calendar Year 2019 APB approved changes and administrative changes	CJIS ISO Program Office	06/01/2020	APB & Compact Council

SUMMARY OF CHANGES

Version 5.9

APB Approved Changes

1. **Section 5.13.2 Mobile Device Management (MDM)**: add clarifying language, Fall 2019, APB#18, SA#3, Mobile Device Management (MDM) Requirements in the *CJIS Security Policy*.
2. **Appendix H, Security Addendum**: add example of contract addendum, Fall 2019, APB#18, SA#7, Audit of Vendor Contracts with Authorized Criminal Justice Agencies (CJAs).
3. **NOTE**: There were no Spring 2019 APB actions.

Administrative Changes[1]

1. **Section 5.6.2.2.2 Advanced Authentication Decision Tree**: updated the tree description to account for direct and indirect access to CJI.
2. **Figures 9 and 10:** updated both figures to account for direct and indirect access to CJI.

KEY TO APB APPROVED CHANGES (e.g. "Fall 2013, APB#11, SA#6, add language, Future CSP for Mobile Devices"):

Fall 2013 – Advisory Policy Board cycle and year

APB# – Advisory Policy Board Topic number

SA# – Security and Access Subcommittee Topic number

Summary of change

Topic title

[1] Administrative changes are vetted through the Security and Access Subcommittee and not the entire APB process.

TABLE OF CONTENTS

Executive Summary ..... **i**
Change Management ..... **ii**
Summary of Changes ..... **iii**
Table of Contents ..... **iv**
List of Figures ..... **ix**
1 Introduction **1**
1.1 Purpose 1
1.2 Scope 1
1.3 Relationship to Local Security Policy and Other Policies 1
1.4 Terminology Used in This Document 2
1.5 Distribution of the CJIS Security Policy 2
2 CJIS Security Policy Approach **3**
2.1 CJIS Security Policy Vision Statement 3
2.2 Architecture Independent 3
2.3 Risk Versus Realism 3
3 Roles and Responsibilities **4**
3.1 Shared Management Philosophy 4
3.2 Roles and Responsibilities for Agencies and Parties 4
3.2.1 CJIS Systems Agencies (CSA) 5
3.2.2 CJIS Systems Officer (CSO) 5
3.2.3 Terminal Agency Coordinator (TAC) 6
3.2.4 Criminal Justice Agency (CJA) 6
3.2.5 Noncriminal Justice Agency (NCJA) 6
3.2.6 Contracting Government Agency (CGA) 7
3.2.7 Agency Coordinator (AC) 7
3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO) 7
3.2.9 Local Agency Security Officer (LASO) 8
3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO) 8
3.2.11 Repository Manager 9
3.2.12 Compact Officer 9
4 Criminal Justice Information and Personally Identifiable Information **10**
4.1 Criminal Justice Information (CJI) 10
4.1.1 Criminal History Record Information (CHRI) 10
4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information 11
4.2.1 Proper Access, Use, and Dissemination of CHRI 11
4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information 11
4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information 11
4.2.3.1 For Official Purposes 11
4.2.3.2 For Other Authorized Purposes 12
4.2.3.3 CSO Authority in Other Circumstances 12
4.2.4 Storage 12
4.2.5 Justification and Penalties 12

4.2.5.1 Justification 12
4.2.5.2 Penalties 12
4.3 Personally Identifiable Information (PII) 12
5 Policy and Implementation 14
5.1 Policy Area 1: Information Exchange Agreements 15
5.1.1 Information Exchange 15
5.1.1.1 Information Handling 15
5.1.1.2 State and Federal Agency User Agreements 15
5.1.1.3 Criminal Justice Agency User Agreements 16
5.1.1.4 Interagency and Management Control Agreements 16
5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum 16
5.1.1.6 Agency User Agreements 17
5.1.1.7 Outsourcing Standards for Channelers 17
5.1.1.8 Outsourcing Standards for Non-Channelers 18
5.1.2 Monitoring, Review, and Delivery of Services 18
5.1.2.1 Managing Changes to Service Providers 18
5.1.3 Secondary Dissemination 18
5.1.4 Secondary Dissemination of Non-CHRI CJI 18
5.2 Policy Area 2: Security Awareness Training 20
5.2.1 Basic Security Awareness Training 20
5.2.1.1 Level One Security Awareness Training 20
5.2.1.2 Level Two Security Awareness Training 20
5.2.1.3 Level Three Security Awareness Training 21
5.2.1.4 Level Four Security Awareness Training 21
5.2.2 LASO Training 22
5.2.3 Security Training Records 22
5.3 Policy Area 3: Incident Response 24
5.3.1 Reporting Security Events 24
5.3.1.1 Reporting Structure and Responsibilities 24
5.3.1.1.1 FBI CJIS Division Responsibilities 24
5.3.1.1.2 CSA ISO Responsibilities 24
5.3.2 Management of Security Incidents 25
5.3.2.1 Incident Handling 25
5.3.2.2 Collection of Evidence 25
5.3.3 Incident Response Training 25
5.3.4 Incident Monitoring 25
5.4 Policy Area 4: Auditing and Accountability 27
5.4.1 Auditable Events and Content (Information Systems) 27
5.4.1.1 Events 27
5.4.1.1.1 Content 28
5.4.2 Response to Audit Processing Failures 28
5.4.3 Audit Monitoring, Analysis, and Reporting 28
5.4.4 Time Stamps 28
5.4.5 Protection of Audit Information 28
5.4.6 Audit Record Retention 28
5.4.7 Logging NCIC and III Transactions 29

5.5 Policy Area 5: Access Control 30
5.5.1 Account Management 30
5.5.2 Access Enforcement 30
5.5.2.1 Least Privilege 31
5.5.2.2 System Access Control 31
5.5.2.3 Access Control Criteria 31
5.5.2.4 Access Control Mechanisms 31
5.5.3 Unsuccessful Login Attempts 32
5.5.4 System Use Notification 32
5.5.5 Session Lock 32
5.5.6 Remote Access 33
5.5.6.1 Personally Owned Information Systems 33
5.5.6.2 Publicly Accessible Computers 33
5.6 Policy Area 6: Identification and Authentication 35
5.6.1 Identification Policy and Procedures 35
5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges 35
5.6.2 Authentication Policy and Procedures 35
5.6.2.1 Standard Authenticators 36
5.6.2.1.1 Password 36
5.6.2.1.2 Personal Identification Number (PIN) 38
5.6.2.1.3 One-time Passwords (OTP) 38
5.6.2.2 Advanced Authentication 38
5.6.2.2.1 Advanced Authentication Policy and Rationale 39
5.6.2.2.2 Advanced Authentication Decision Tree 39
5.6.3 Identifier and Authenticator Management 41
5.6.3.1 Identifier Management 41
5.6.3.2 Authenticator Management 42
5.6.4 Assertions 42
5.7 Policy Area 7: Configuration Management 48
5.7.1 Access Restrictions for Changes 48
5.7.1.1 Least Functionality 48
5.7.1.2 Network Diagram 48
5.7.2 Security of Configuration Documentation 48
5.8 Policy Area 8: Media Protection 49
5.8.1 Media Storage and Access 49
5.8.2 Media Transport 49
5.8.2.1 Digital Media during Transport 49
5.8.2.2 Physical Media in Transit 49
5.8.3 Digital Media Sanitization and Disposal 49
5.8.4 Disposal of Physical Media 49
5.9 Policy Area 9: Physical Protection 51
5.9.1 Physically Secure Location 51
5.9.1.1 Security Perimeter 51
5.9.1.2 Physical Access Authorizations 51
5.9.1.3 Physical Access Control 51

5.9.1.4 Access Control for Transmission Medium 51
5.9.1.5 Access Control for Display Medium 51
5.9.1.6 Monitoring Physical Access 52
5.9.1.7 Visitor Control 52
5.9.1.8 Delivery and Removal 52
5.9.2 Controlled Area 52
5.10 Policy Area 10: System and Communications Protection and Information Integrity 53
5.10.1 Information Flow Enforcement 53
5.10.1.1 Boundary Protection 53
5.10.1.2 Encryption 54
5.10.1.2.1 Encryption for CJI in Transit 54
5.10.1.2.2 Encryption for CJI at Rest 55
5.10.1.2.3 Public Key Infrastructure (PKI) Technology 55
5.10.1.3 Intrusion Detection Tools and Techniques 55
5.10.1.4 Voice over Internet Protocol 56
5.10.1.5 Cloud Computing 56
5.10.2 Facsimile Transmission of CJI 57
5.10.3 Partitioning and Virtualization 57
5.10.3.1 Partitioning 57
5.10.3.2 Virtualization 58
5.10.4 System and Information Integrity Policy and Procedures 58
5.10.4.1 Patch Management 58
5.10.4.2 Malicious Code Protection 59
5.10.4.3 Spam and Spyware Protection 59
5.10.4.4 Security Alerts and Advisories 59
5.10.4.5 Information Input Restrictions 60
5.11 Policy Area 11: Formal Audits 61
5.11.1 Audits by the FBI CJIS Division 61
5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division 61
5.11.1.2 Triennial Security Audits by the FBI CJIS Division 61
5.11.2 Audits by the CSA 61
5.11.3 Special Security Inquiries and Audits 62
5.11.4 Compliance Subcommittees 62
5.12 Policy Area 12: Personnel Security 63
5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI 63
5.12.2 Personnel Termination 64
5.12.3 Personnel Transfer 64
5.12.4 Personnel Sanctions 64
5.13 Policy Area 13: Mobile Devices 66
5.13.1 Wireless Communications Technologies 66
5.13.1.1 802.11 Wireless Protocols 66
5.13.1.2 Cellular Devices 67
5.13.1.2.1 Cellular Service Abroad 68
5.13.1.2.2 Voice Transmissions Over Cellular Devices 68
5.13.1.3 Bluetooth 68

5.13.1.4 Mobile Hotspots 68
5.13.2 Mobile Device Management (MDM) 69
5.13.3 Wireless Device Risk Mitigations 69
5.13.4 System Integrity 70
5.13.4.1 Patching/Updates 70
5.13.4.2 Malicious Code Protection 70
5.13.4.3 Personal Firewall 70
5.13.5 Incident Response 71
5.13.6 Access Control 71
5.13.7 Identification and Authentication 71
5.13.7.1 Local Device Authentication 71
5.13.7.2 Advanced Authentication 72
5.13.7.2.1 Compensating Controls 72
5.13.7.3 Device Certificates 72
Appendices A-1
Appendix A Terms and Definitions A-1
Appendix B Acronyms B-1
Appendix C Network Topology Diagrams C-1
Appendix D Sample Information Exchange Agreements D-1
D.1 CJIS User Agreement D-1
D.2 Management Control Agreement D-9
D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding D-10
D.4 Interagency Connection Agreement D-16
Appendix E Security Forums and Organizational Entities E-1
Appendix F Sample Forms F-1
F.1 Security Incident Response Form F-2
Appendix G Best practices G-1
G.1 Virtualization G-1
G.2 Voice over Internet Protocol G-4
G.3 Cloud Computing G-15
G.4 Mobile Appendix G-32
G.5 Administrator Accounts for Least Privilege and Separation of Duties G-53
G.6 Encryption G-66
G.7 Incident Response G-76
G.8 Secure Coding G-89
Appendix H Security Addendum H-1
Appendix I References I-1
Appendix J Noncriminal Justice Agency Supplemental Guidance J-1
Appendix K Criminal Justice Agency Supplemental Guidance K-1

LIST OF FIGURES

Figure 1 – Overview Diagram of Strategic Functions and Policy Components....4
Figure 2 – Dissemination of restricted and non-restricted NCIC data....13
Figure 3 – Information Exchange Agreements Implemented by a Local Police Department....19
Figure 4 – Security Awareness Training Use Cases....22
Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department....26
Figure 6 – Local Police Department's Use of Audit Logs....29
Figure 7 – A Local Police Department's Access Controls....34
Figure 8 – Advanced Authentication Use Cases....42
Figure 9 – Authentication Decision for Known Location....46
Figure 10 – Authentication Decision for Unknown Location....47
Figure 11 – A Local Police Department's Configuration Management Controls....48
Figure 12 – A Local Police Department's Media Management Policies....50
Figure 13 – A Local Police Department's Physical Protection Measures....52
Figure 14 – System and Communications Protection and Information Integrity Use Cases....60
Figure 15 – The Audit of a Local Police Department....62
Figure 16 – A Local Police Department's Personnel Security Controls....64

1 INTRODUCTION

This section details the purpose of this document, its scope, relationship to other information security policies, and its distribution constraints.

1.1 Purpose

The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) and the National Crime Prevention and Privacy Compact Council (Compact Council).

1.2 Scope

At the consent of the advisory process, and taking into consideration federal law and state statutes, the CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The CJIS Security Policy provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Entities engaged in the interstate exchange of CJI data for noncriminal justice purposes are also governed by the standards and rules promulgated by the Compact Council.

1.3 Relationship to Local Security Policy and Other Policies

The CJIS Security Policy may be used as the sole security policy for the agency. The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for CJIS Security Policy areas can be developed for the security program in general, and for a particular information system, when required.

This document is a compendium of applicable policies in providing guidance on the minimum security controls and requirements needed to access FBI CJIS information and services. These policies include presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions. State, local, and Tribal CJA may implement more stringent policies

and requirements. Appendix I contains the references while Appendix E lists the security forums and organizational entities referenced in this document.

1.4 Terminology Used in This Document

The following terms are used interchangeably throughout this document:

- Agency and Organization: The two terms in this document refer to any entity that submits or receives information, by any means, to/from FBI CJIS systems or services.
- Information and Data: Both terms refer to CJI.
- System, Information System, Service, or named applications like NCIC: all refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections.
- References/Citations/Directives: Appendix I contains all of the references used in this Policy and may contain additional sources that could apply to any section.

Appendix A and B provide an extensive list of the terms and acronyms.

1.5 Distribution of the CJIS Security Policy

The CJIS Security Policy, version 5.0 and later, is a publically available document and may be posted and shared without restrictions.

2 CJIS SECURITY POLICY APPROACH

The CJIS Security Policy represents the shared responsibility between FBI CJIS, CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJI. The Policy provides a baseline of security requirements for current and planned services and sets a minimum standard for new initiatives.

2.1 CJIS Security Policy Vision Statement

The executive summary of this document describes the vision in terms of business needs for confidentiality, integrity, and availability of information. The APB collaborates with the FBI CJIS Division to ensure that the Policy remains updated to meet evolving business, technology and security needs.

2.2 Architecture Independent

Due to advancing technology and evolving business models, the FBI CJIS Division is transitioning from legacy stovepipe systems and moving toward a flexible services approach. Systems such as National Crime Information Center (NCIC), National Instant Criminal Background Check System (NICS), and Next Generation Identification (NGI) will continue to evolve and may no longer retain their current system platforms, hardware, or program name. However, the data and services provided by these systems will remain stable.

The CJIS Security Policy looks at the data (information), services, and protection controls that apply regardless of the implementation architecture. Architectural independence is not intended to lessen the importance of systems, but provide for the replacement of one technology with another while ensuring the controls required to protect the information remain constant. This objective and conceptual focus on security policy areas provide the guidance and standards while avoiding the impact of the constantly changing landscape of technical innovations. The architectural independence of the Policy provides agencies with the flexibility for tuning their information security infrastructure and policies to reflect their own environments.

2.3 Risk Versus Realism

Every "shall" statement contained within the CJIS Security Policy has been scrutinized for risk versus the reality of resource constraints and real-world application. The purpose of the CJIS Security Policy is to establish the minimum security requirements; therefore, individual agencies are encouraged to implement additional controls to address agency specific risks. Each agency faces risk unique to that agency. It is quite possible that several agencies could encounter the same type of risk however depending on resources would mitigate that risk differently. In that light, a risk-based approach can be used when implementing requirements.

3 ROLES AND RESPONSIBILITIES

3.1 Shared Management Philosophy

In the scope of information security, the FBI CJIS Division employs a shared management philosophy with federal, state, local, and tribal law enforcement agencies. Although an advisory policy board for the NCIC has existed since 1969, the Director of the FBI established the CJIS APB in March 1994 to enable appropriate input and recommend policy with respect to CJIS services. Through the APB and its Subcommittees and Working Groups, consideration is given to the needs of the criminal justice and law enforcement community regarding public policy, statutory and privacy aspects, as well as national security relative to CJIS systems and information. The APB represents federal, state, local, and tribal law enforcement and criminal justice agencies throughout the United States, its territories, and Canada.

The FBI has a similar relationship with the Compact Council, which governs the interstate exchange of criminal history records for noncriminal justice purposes. The Compact Council is mandated by federal law to promulgate rules and procedures for the use of the Interstate Identification Index (III) for noncriminal justice purposes. To meet that responsibility, the Compact Council depends on the CJIS Security Policy as the definitive source for standards defining the security and privacy of records exchanged with noncriminal justice practitioners.

3.2 Roles and Responsibilities for Agencies and Parties

It is the responsibility of all agencies covered under this Policy to ensure the protection of CJI between the FBI CJIS Division and its user community. The following figure provides an abstract representation of the strategic functions and roles such as governance and operations.

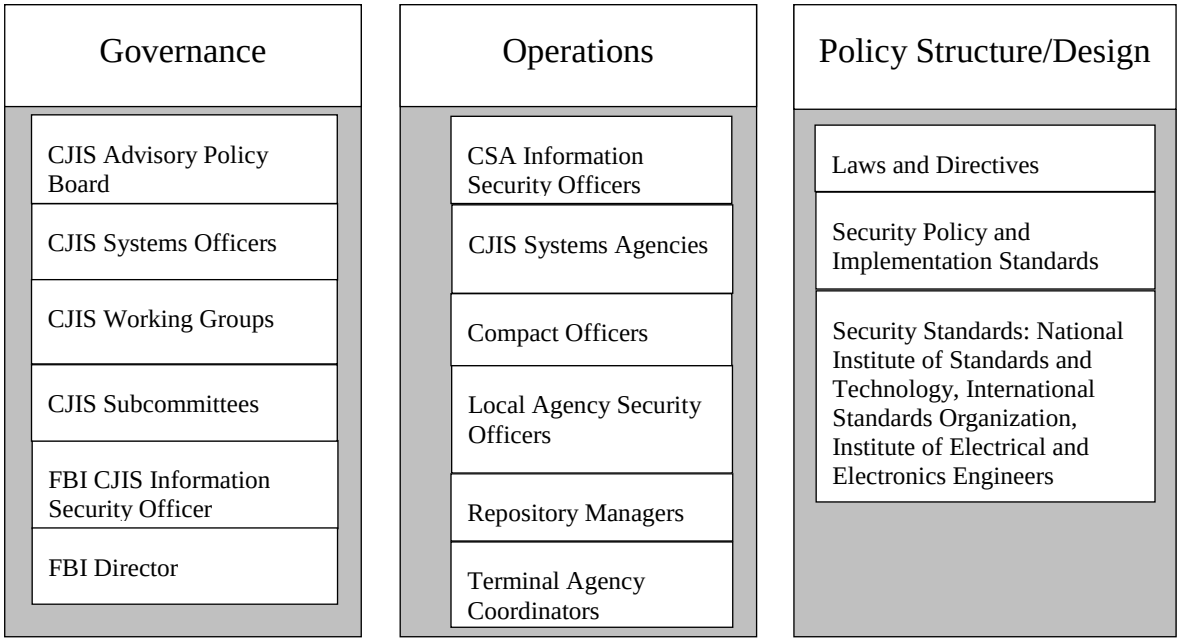


Figure 1 – Overview Diagram of Strategic Functions and Policy Components

This section provides a description of the following entities and roles:

1. CJIS Systems Agency.
2. CJIS Systems Officer.
3. Terminal Agency Coordinator.
4. Criminal Justice Agency.
5. Noncriminal Justice Agency.
6. Contracting Government Agency.
7. Agency Coordinator.
8. CJIS Systems Agency Information Security Officer.
9. Local Agency Security Officer.
10. FBI CJIS Division Information Security Officer.
11. Repository Manager.
12. Compact Officer.

3.2.1 CJIS Systems Agencies (CSA)

The CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include the local levels. The head of each CSA shall appoint a CJIS Systems Officer (CSO). The CSA may impose more stringent protection measures than outlined in this document. Such decisions shall be documented and kept current.

3.2.2 CJIS Systems Officer (CSO)

The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. Pursuant to the Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced. The CSO may delegate responsibilities to subordinate agencies. The CSO shall set, maintain, and enforce the following:

1. Standards for the selection, supervision, and separation of personnel who have access to CJI.
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.
    a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
    b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.

c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.

d. Ensure the designation of a Terminal Agency Coordinator (TAC) within each agency with devices accessing CJIS systems.

e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).

f. Ensure each LASO receives enhanced security awareness training (ref. Section 5.2).

g. Approve access to FBI CJIS systems.

h. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.

i. Perform other related duties outlined by the user agreements with the FBI CJIS Division.

3. Outsourcing of Criminal Justice Functions

a. Responsibility for the management of the approved security requirements shall remain with the CJA. Security control includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit CJI; and to guarantee the priority service needed by the criminal justice community.

b. Responsibility for the management control of network security shall remain with the CJA. Management control of network security includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of circuits and network equipment used to transmit CJI; and to guarantee the priority service as determined by the criminal justice community.

3.2.3 Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

3.2.4 Criminal Justice Agency (CJA)

A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

3.2.5 Noncriminal Justice Agency (NCJA)

A NCJA is defined (for the purposes of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

3.2.6 Contracting Government Agency (CGA)

A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC)

An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
2. Participate in related meetings and provide input and comments for system improvement.
3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.
7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
10. Any other responsibility for the AC promulgated by the FBI.

3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.

2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)

The FBI CJIS ISO shall:

1. Maintain the CJIS Security Policy.
2. Disseminate the FBI Director approved CJIS Security Policy.
3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.
4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.
7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.

3.2.11 Repository Manager

The State Identification Bureau (SIB) Chief, i.e. Repository Manager or Chief Administrator, is the designated manager of the agency having oversight responsibility for a state's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

3.2.12 Compact Officer

Pursuant to the National Crime Prevention and Privacy Compact, each party state shall appoint a Compact Officer who shall ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.

4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. Identity History Data—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. Case/Incident History—information about the history of criminal incidents.

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g. within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules. CJI introduced into the court system pursuant to a judicial proceeding that can be released to the public via a public records request is not subject to the CJIS Security Policy.

4.1.1 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI), sometimes informally referred to as "restricted data", is a subset of CJI. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.

4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information

This section describes the requirements for the access, use and dissemination of CHRI, NCIC restricted files information, and NCIC non-restricted files information.

4.2.1 Proper Access, Use, and Dissemination of CHRI

Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.

4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information

The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows:

1. Gang Files
2. Known or Appropriately Suspected Terrorist Files
3. Supervised Release Files
4. National Sex Offender Registry Files
5. Historical Protection Order Files of the NCIC
6. Identity Theft Files
7. Protective Interest Files
8. Person With Information (PWI) data in the Missing Person Files
9. Violent Person File
10. NICS Denied Transactions File

The remaining NCIC files are considered non-restricted files.

4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information

4.2.3.1 For Official Purposes

NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with

the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

4.2.3.2 For Other Authorized Purposes

NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially.

A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.

4.2.3.3 CSO Authority in Other Circumstances

If no federal, state or local law or policy prohibition exists, the CSO may exercise discretion to approve or deny dissemination of NCIC non-restricted file information.

4.2.4 Storage

When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files. See Section 5.9 for physical security controls.

4.2.5 Justification and Penalties

4.2.5.1 Justification

In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.

4.2.5.2 Penalties

Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

4.3 Personally Identifiable Information (PII)

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for

example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

Figure 2 – Dissemination of restricted and non-restricted NCIC data

A citizen of Springfield went to the Springfield Police Department to request whether his new neighbor, who had been acting suspiciously, had an outstanding warrant. The Springfield Police Department ran an NCIC persons inquiry, which produced a response that included a Wanted Person File (non-restricted file) record and a Known or Appropriately Suspected Terrorist File (restricted file) record. The Springfield Police Department advised the citizen of the outstanding warrant, but did not disclose any information concerning the subject being a known or appropriately suspected terrorist.

5 POLICY AND IMPLEMENTATION

The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances. The policy areas are:

- Policy Area 1—Information Exchange Agreements
- Policy Area 2—Security Awareness Training
- Policy Area 3—Incident Response
- Policy Area 4—Auditing and Accountability
- Policy Area 5—Access Control
- Policy Area 6—Identification and Authentication
- Policy Area 7—Configuration Management
- Policy Area 8—Media Protection
- Policy Area 9—Physical Protection
- Policy Area 10—Systems and Communications Protection and Information Integrity
- Policy Area 11—Formal Audits
- Policy Area 12—Personnel Security
- Policy Area 13—Mobile Devices

5.1 Policy Area 1: Information Exchange Agreements

The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

5.1.1 Information Exchange

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.

Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.

There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.

5.1.1.1 Information Handling

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange.

The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including – but not limited to - employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

5.1.1.2 State and Federal Agency User Agreements

Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs. This agreement shall include the standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA

or SIB Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system. All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.

5.1.1.3 Criminal Justice Agency User Agreements

Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:

1. Audit.
2. Dissemination.
3. Hit confirmation.
4. Logging.
5. Quality Assurance (QA).
6. Screening (Pre-Employment).
7. Security.
8. Timeliness.
9. Training.
10. Use of the system.
11. Validation.

5.1.1.4 Interagency and Management Control Agreements

A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an interagency agreement. An example of an NCJA (government) is a city information technology (IT) department.

5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum

The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security

Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

5.1.1.6 Agency User Agreements

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (private) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

5.1.1.7 Outsourcing Standards for Channelers

Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact

Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing.

Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.1.8 Outsourcing Standards for Non-Channelers

Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.2 Monitoring, Review, and Delivery of Services

As specified in the interagency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.

5.1.2.1 Managing Changes to Service Providers

Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

5.1.3 Secondary Dissemination

If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

5.1.4 Secondary Dissemination of Non-CHRI CJI

If CJI does not contain CHRI and is not part of an information exchange agreement then it does not need to be logged. Dissemination shall conform to the local policy validating the requestor of the CJI as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.

Figure 3 – Information Exchange Agreements Implemented by a Local Police Department

A local police department executed a Memorandum of Understanding (MOU) for the interface with their state CSA. The local police department also executed an MOU (which included an MCA) with the county information technology (IT) department for the day-to-day operations of their criminal-justice infrastructure. The county IT department, in turn, outsourced operations to a local vendor who signed the CJIS Security Addendum.

5.2 Policy Area 2: Security Awareness Training

Security training is key to the human element of information security. All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI. LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.

5.2.1 Basic Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location. The CSO/SIB Chief may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

5.2.1.1 Level One Security Awareness Training

At a minimum, the following topics shall be addressed as baseline security awareness training for all personnel who have unescorted access to a physically secure location:

1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals.
2. Implications of noncompliance.
3. Incident response (Identify points of contact and individual actions).
4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

5.2.1.2 Level Two Security Awareness Training

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Media protection.
2. Protect information subject to confidentiality concerns — hardcopy through destruction.
3. Proper handling and marking of CJI.
4. Threats, vulnerabilities, and risks associated with handling of CJI.
5. Social engineering.
6. Dissemination and destruction.

5.2.1.3 Level Three Security Awareness Training

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to information system usage.
2. Password usage and management—including creation, frequency of changes, and protection.
3. Protection from viruses, worms, Trojan horses, and other malicious code.
4. Unknown e-mail/attachments.
5. Web usage—allowed versus prohibited; monitoring of user activity.
6. Spam.
7. Physical Security—increases in risks to systems and data.
8. Handheld device security issues—address both physical and wireless security issues.
9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
10. Laptop security—address both physical and information security issues.
11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
12. Access control issues—address least privilege and separation of duties.
13. Individual accountability—explain what this means in the agency.
14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.
16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

5.2.1.4 Level Four Security Awareness Training

In addition to 5.2.1.1, 5.2.1.2, and 5.1.2.3 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
2. Data backup and storage—centralized or decentralized approach.

3. Timely application of system patches—part of configuration management.
4. Access control measures.
5. Network infrastructure protection measures.

5.2.2 LASO Training

LASO training shall be required prior to assuming duties but no later than six months after initial assignment, and annually thereafter.

At a minimum, the following topics shall be addressed as enhanced security awareness training for a LASO:

1. The roles and responsibilities listed in CJIS Security Policy Section 3.2.9.
2. Additional state/local/tribal/federal agency LASO roles and responsibilities.
3. Summary of audit findings from previous state audits of local agencies.
4. Findings from the last FBI CJIS Division audit of the CSA.
5. Most recent changes to the CJIS Security Policy.

5.2.3 Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB Chief/Compact Officer. Maintenance of training records can be delegated to the local level.

Figure 4 – Security Awareness Training Use Cases

Use Case 1 - Security Awareness Training Program Implementation by a Local Police Department

A local police department with a staff of 20 sworn criminal justice professionals and 15 support personnel worked with a vendor to develop role-specific security-awareness training, and required all staff to complete this training upon assignment and every two years thereafter. The local police department scheduled the sworn law-enforcement training to coincide with their NCIC certification training. The vendor maintained the training records for the police department's entire staff, and provided reporting to the department to help it ensure compliance with the CJIS Security Policy.

Use Case 2 - Level One Security Awareness Training

A local police department hires custodial staff that will have physical access throughout the PD (a physically secure location) after normal business hours to clean the facility. These personnel have unescorted access to a physically secure location and therefore must be given the baseline security awareness training on all the topics identified in CSP Section 5.2.1.1 Level One Security Awareness Training.

Use Case 3 – Level Two Security Awareness Training

A school district maintains a locked file cabinet with hard copies of background check results of all teachers and employees which may include CJI (CHRI). Only authorized personnel who have the

ability to open the cabinet are required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1 and 5.2.1.2.

Use Case 4 – Level Three Security Awareness Training

A County Sheriff's Office has employed a number of dispatchers. Part of the function of these dispatchers is to run CJI queries at the request of the Sheriff and deputies. As part of their daily duties, the dispatchers have access to CJI both logically (running queries) and physically (printed copies of reports containing CJI). These dispatchers are entrusted with direct access to CJI and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, and 5.2.1.3.

Use Case 5 – Level Four Security Awareness Training

The State Police has hired a number of system and network administrator personnel to help bolster security of the state network. Part of their daily duties may include creating accounts for new personnel, implementing security patches for existing systems, creating backups of existing systems, and implementing access controls throughout the network. These administrators have privileged access to CJI and CJI-processing systems, and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, 5.2.1.3, and 5.2.1.4.

5.3 Policy Area 3: Incident Response

The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F contains a sample incident notification letter for use when communicating the details of a CJI-related incident to the FBI CJIS ISO.

Refer to Section 5.13.5 for additional incident response requirements related to mobile devices used to access CJI.

5.3.1 Reporting Security Events

The agency shall promptly report incident information to appropriate authorities. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

5.3.1.1 Reporting Structure and Responsibilities

5.3.1.1.1 FBI CJIS Division Responsibilities

The FBI CJIS Division shall:

1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
4. Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on FBI.gov, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
5. Track all reported incidents and/or trends.
6. Monitor the resolution of all incidents.

5.3.1.1.2 CSA ISO Responsibilities

The CSA ISO shall:

1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
6. Act as a single POC for their jurisdictional area for requesting incident response assistance.

5.3.2 Management of Security Incidents

A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.

5.3.2.1 Incident Handling

The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

5.3.2.2 Collection of Evidence

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

5.3.3 Incident Response Training

The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.

5.3.4 Incident Monitoring

The agency shall track and document security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department

A state ISO received a notification from a local police department that suspicious network activity from a known botnet was detected on their network. The state ISO began the process of collecting all pertinent information about this incident, e.g. incident date/time, points-of-contact, systems affected, nature of the incident, actions taken, etc. and requested that the local police department confirm that their malware signatures were up to date. The state ISO contacted both the FBI CJIS ISO and state CSO to relay the preliminary details of this incident. The FBI CJIS ISO instructed the involved parties to continue their investigation and to submit an incident response form once all the information had been gathered. The FBI CJIS ISO contacted the lead for the FBI CSIRC to inform them that an incident response form was forthcoming. The state ISO gathered the remainder of the information from the local police department and submitted a completed incident response form to the FBI CJIS ISO who subsequently provided it to the FBI CSIRC. The FBI CSIRC notified the Department of Justice Computer Incident Response Team (DOJCIRT). The state ISO continued to monitor the situation, passing relevant details to the FBI CJIS ISO, ultimately determining that the botnet was eliminated from the local police department's infrastructure. Subsequent investigations determined that the botnet was restricted to the department's administrative infrastructure and thus no CJI was compromised.

5.4 Policy Area 4: Auditing and Accountability

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.

Refer to Section 5.13.6 for additional audit requirements related to mobile devices used to access CJI.

5.4.1 Auditable Events and Content (Information Systems)

The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems.

The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.

5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
    a. access permission on a user account, file, directory or other system resource;
    b. create permission on a user account, file, directory or other system resource;
    c. write permission on a user account, file, directory or other system resource;
    d. delete permission on a user account, file, directory or other system resource;
    e. change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts (i.e. root, Oracle, DBA, admin, etc.).
5. Successful and unsuccessful attempts for users to:
    a. access the audit log file;

b. modify the audit log file;

c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

5.4.2 Response to Audit Processing Failures

The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

5.4.3 Audit Monitoring, Analysis, and Reporting

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

5.4.4 Time Stamps

The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.

5.4.5 Protection of Audit Information

The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

5.4.6 Audit Record Retention

The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for

example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

5.4.7 Logging NCIC and III Transactions

A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.

Figure 6 – Local Police Department's Use of Audit Logs

A state CSO contacted a local police department regarding potentially inappropriate use of CHRI that was retrieved using the local department's ORI. The state CSO requested all relevant information from the police department to reconcile state NCIC and III logs against local police department logs. The police department provided the combination of their CJI processing application's logs with relevant operating system and network infrastructure logs to help verify the identity of the users conducting these queries. The review of these logs substantiated the CSO's suspicion.

5.5 Policy Area 5: Access Control

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

Refer to Section 5.13.6 for additional access control requirements related to mobile devices used to access CJI.

5.5.1 Account Management

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The agency responsible for account creation shall be notified when:

1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

5.5.2 Access Enforcement

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

5.5.2.1 Least Privilege

The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.

Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.

5.5.2.2 System Access Control

Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to:

1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.
2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

5.5.2.3 Access Control Criteria

Agencies shall control access to CJI based on one or more of the following:

1. Job assignment or function (i.e., the role) of the user seeking access.
2. Physical location.
3. Logical location.
4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
5. Time-of-day and day-of-week/month restrictions.

5.5.2.4 Access Control Mechanisms

When setting up access controls, agencies shall use one or more of the following mechanisms:

1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.
2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.

3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. Follow the guidance in Section 5.10.1.2 for encryption requirements if encryption of stored information is employed as an access enforcement mechanism.
4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.

5.5.3 Unsuccessful Login Attempts

Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.

5.5.4 System Use Notification

The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is accessing a restricted information system.
2. System usage may be monitored, recorded, and subject to audit.
3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
4. Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems:

1. the system use information is available and when appropriate, is displayed before granting access;
2. any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and
3. the notice given to public users of the information system includes a description of the authorized uses of the system.

5.5.5 Session Lock

The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall

directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e. receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement. Note: an example of a session lock is a screen saver with password.

5.5.6 Remote Access

The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system.

Virtual escorting of privileged functions is permitted only when all the following conditions are met:

1. The session shall be monitored at all times by an authorized escort
2. The escort shall be familiar with the system/area in which the work is being performed.
3. The escort shall have the ability to end the session at any time.
4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

5.5.6.1 Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices.

This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

5.5.6.2 Publicly Accessible Computers

Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Figure 7 – A Local Police Department's Access Controls

A local police department purchased a new computer-assisted dispatch (CAD) system that integrated with their state CSA's CJI interfaces. In doing so, the police department employed least-privilege practices to ensure that its employees were only given those privileges needed to perform their jobs, and as such, excluding IT administrators, employees had only non-administrative privileges on all equipment they used. The police department also used ACLs in the operating systems to control access to the CAD client's executables. The CAD system used internal role-based access controls to ensure only those users that needed access to CJI were given it. The police department performed annual audits of user accounts on all systems under their control including remote access mechanisms, operating systems, and the CAD system to ensure all accounts were in valid states. The police department implemented authentication-failure account lockouts, system use notification via login banners, and screen-saver passwords on all equipment that processes CJI.

5.6 Policy Area 6: Identification and Authentication

The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.

5.6.1 Identification Policy and Procedures

Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges

An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.

Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.

Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.

5.6.2 Authentication Policy and Procedures

Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The CSA/SIB may develop an authentication strategy which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI.

Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance. The FBI CJIS Division shall identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services. The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not

further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.

5.6.2.1 Standard Authenticators

Authenticators are (the something you know, something you are, or something you have) part of the identification and authentication process. Examples of standard authenticators include passwords, hard or soft tokens, biometrics, one-time passwords (OTP) and personal identification numbers (PIN). Users shall not be allowed to use the same password or PIN in the same logon sequence.

5.6.2.1.1 Password

When agencies use a password as an authenticator for an individual's unique ID, they shall use the basic password standards in 5.6.2.1.1.1, OR follow the advanced password standards in 5.6.2.1.1.2.

NOTE: There is no option to combine or select particular options between the two separate lists below.

5.6.2.1.1.1 Basic Password Standards

When agencies elect to follow the basic password standards, passwords shall:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the Userid.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

5.6.2.1.1.2 Advanced Password Standards

When agencies elect to follow the advanced password standards, passwords shall:

1. Passwords shall be a minimum of twenty (20) characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).
2. Password Verifiers shall not permit the use of a stored "hint" for forgotten passwords and/or prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing a password.
3. Verifiers shall maintain a list of "banned passwords" that contains values known to be commonly-used, expected, or compromised. For example, the list may include, but is not limited to:

a. Passwords obtained from previous breach corpuses

b. Dictionary words

c. Repetitive or sequential characters (e.g. ‘aaaaaa’, ‘1234abcd’)

d. Context-specific words, such as the name of the service, the username, and derivatives thereof

4. When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the “banned passwords” list.
5. If the chosen password is found to be part of a “banned passwords” list, the Verifier shall:
   a. Advise the subscriber that they need to select a different password,
   b. Provide the reason for rejection, and
   c. Require the subscriber to choose a different password.
6. Verifiers shall limit the number of failed authentication attempts that can be made as described in Section 5.5.3 Unsuccessful Login Attempts.
7. Verifiers shall force a password change if there is evidence of authenticator compromise or every 365 days from the last password change.
8. Verifiers shall use approved encryption and an authenticated protected channel when requesting passwords to protect against eavesdropping and Man-in-the-Middle (MitM) attacks.
9. Verifiers shall store passwords in a manner that is resistant to offline attacks by salting and hashing the password using a one-way key derivation function when stored.
   a. The salt shall be at least 32 bits in length.
   b. The salt shall be chosen arbitrarily so as to minimize salt value collisions among stored hashes.

   Note: Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive.
10. For each subscriber, Verifiers shall protect stored salt and resulting hash values using a password or PIN.

5.6.2.1.2 Personal Identification Number (PIN)

When agencies implement the use of a PIN as a standard authenticator, the PIN attributes shall follow the guidance in section 5.6.2.1.1 (password). When agencies utilize a PIN in conjunction with a certificate or a token (e.g. key fob with rolling numbers) for the purpose of advanced authentication, agencies shall follow the PIN attributes described below. For example: A user certificate is installed on a smartphone for the purpose of advanced authentication (AA). As the user invokes that certificate, a PIN meeting the below attributes shall be used to access the certificate for the AA process.

1. Be a minimum of six (6) digits
2. Have no repeating digits (i.e., 112233)
3. Have no sequential patterns (i.e., 123456)
4. Not be the same as the Userid.
5. Expire within a maximum of 365 calendar days.
    a. If a PIN is used to access a soft certificate which is the second factor of authentication, AND the first factor is a password that complies with the requirements in Section 5.6.2.1.1, then the 365 day expiration requirement can be waived by the CSO.
6. Not be identical to the previous three (3) PINs.
7. Not be transmitted in the clear outside the secure location.
8. Not be displayed when entered.

EXCEPTION: When a PIN is used for local device authentication, the only requirement is that it be a minimum of six (6) digits.

5.6.2.1.3 One-time Passwords (OTP)

One-time passwords are considered a “something you have” token for authentication. Examples include bingo cards, hard or soft tokens, and out-of-band tokens (i.e. OTP received via a text message).

When agencies implement the use of an OTP as an authenticator, the OTP shall meet the requirements described below.

1. Be a minimum of six (6) randomly generated characters
2. Be valid for a single session
3. If not used, expire within a maximum of five (5) minutes after issuance

5.6.2.2 Advanced Authentication

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, out-of-band authenticators (retrieved via a separate communication service channel – e.g., authenticator is sent on demand via text message, phone call, etc.), or “Risk-based Authentication” that includes a software token element comprised of a number of factors, such as

network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

When user-based certificates are used for authentication purposes, they shall:

1. Be specific to an individual user and not to a particular device.
2. Prohibit multiple users from utilizing the same certificate.
3. Require the user to "activate" that certificate for each use in some manner (e.g., passphrase or user-specific PIN).

5.6.2.2.1 Advanced Authentication Policy and Rationale

The requirement to use or not use AA is dependent upon the physical, personnel, and technical security controls associated with the user location and whether CJI is accessed directly or indirectly. AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access). Conversely, if the technical security controls have not been met, AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions. The CSO will make the final determination of whether access is considered indirect.

The intent of AA is to meet the standards of two-factor authentication. Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

EXCEPTION:

AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access. EXAMPLES:

1. A user, irrespective of his/her location, accesses the LEEP portal. The LEEP has AA built into its services and requires AA prior to granting access. AA is required.
2. A user, irrespective of their location, accesses a State's portal through which access to CJI is facilitated. The State Portal has AA built into its processes and requires AA prior to granting access. AA is required.

5.6.2.2.2 Advanced Authentication Decision Tree

The following AA Decision Tree, coupled with figures 9 and 10 below, assists decision makers in determining whether or not AA is required.

1. Is the access to CJI direct access or indirect access?
    a. If access is direct, proceed to question 2.
    b. If access is indirect, decision tree is completed. AA is not required.
2. Can request's physical originating location be determined?

If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 3.

a. The IP address is attributed to a physical structure; or

b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure.

If neither (a) or (b) above are true then the answer is "no". Skip to question number 5.

3. Does request originate from within a physically secure location as described in Section 5.9.1?

   If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 4.

   a. The IP address is attributed to a physically secure location; or

   b. If a mnemonic is used it is attributed to a specific device assigned to a specific physically secure location.

   If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.

4. Are all required technical controls implemented at this location or at the controlling agency?

   If either (a) or (b) below are true the answer to the above question is "yes". Decision tree completed. AA is not required.

   a. Appropriate technical controls listed in Sections 5.5 and 5.10 are implemented; or

   b. The controlling agency (i.e. parent agency or agency leveraged as conduit to CJI) extends its wide area network controls down to the requesting agency and the extended controls provide assurance equal or greater to the controls listed in Sections 5.5 and 5.10.

   If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.

5. Does request originate from an agency-controlled user device?

   If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 6.

   a. The static IP address or MAC address can be traced to registered device; or

   b. Certificates are issued to agency managed devices only and certificate exchange is allowed only between authentication server and agency issued devices.

   If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.

6. Is the agency managed user device associated with and located within a criminal justice conveyance?

If any of the (a), (b), or (c) statements below is true the answer to the above question is "yes". Proceed to Figure 9 Step 4.

a. The static IP address or MAC address is associated with a device associated with a criminal justice conveyance; or

b. The certificate presented is associated with a device associated with a criminal justice conveyance; or

c. The mnemonic presented is associated with a specific device assigned and that device is attributed to a criminal justice conveyance.

If none of the (a), (b), or (c) statements above are true then the answer is "no". Proceed to question number 7.

7. Is the user device an agency-issued and controlled smartphone or tablet?

   If both (a) and (b) below are true, the answer to the above question is "yes." Proceed to question number 8.

   a. The law enforcement agency issued the device to an individual; and

   b. The device is subject to administrative management control of the issuing agency.

   If either (a) or (b) above is false, then the answer is "no." Decision tree completed. AA required.

8. Does the agency-issued smartphone or tablet have CSO-approved AA compensating controls implemented?

   If (a) and (b) below are true, the answer to the above question is "yes." Decision tree completed. AA is not required.

   a. An agency cannot meet a requirement due to legitimate technical or business constraints; and

   b. The CSO has given written approval permitting temporary AA compensating controls to be implemented in lieu of the required AA control measures.

   If either (a) or (b) above is false then the answer is "no." Decision tree completed. AA required.

5.6.3 Identifier and Authenticator Management

The agency shall establish identifier and authenticator management processes.

5.6.3.1 Identifier Management

In order to manage user identifiers, agencies shall:

1. Uniquely identify each user.
2. Verify the identity of each user.
3. Receive authorization to issue a user identifier from an appropriate agency official.
4. Issue the user identifier to the intended party.

5. Disable the user identifier after a specified period of inactivity.
6. Archive user identifiers.

5.6.3.2 Authenticator Management

In order to manage information system authenticators, agencies shall:

1. Define initial authenticator content.
2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
3. Change default authenticators upon information system installation.
4. Change/refresh authenticators periodically.

Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

5.6.4 Assertions

Identity providers can be leveraged to identify individuals and assert the individual's identity to a service or to a trusted broker who will in-turn assert the identity to a service. Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be:

1. Digitally signed by a trusted entity (e.g., the identity provider).
2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.

Assertions generated by a verifier shall expire after 12 hours and shall not be accepted thereafter by the relying party.

Figure 8 – Advanced Authentication Use Cases

Use Case 1 - A Local Police Department Authentication Control Scenario

During the course of an investigation, a detective attempts to access Criminal Justice Information (CJI) from a hotel room using an agency issued mobile broadband card. To gain access, the detective first establishes the remote session via a secure virtual private network (VPN) tunnel (satisfying the requirement for encryption). Upon connecting to the agency network, the detective is challenged for a username (identification), password ("something you know"), and a one-time password OTP ("something you have") from a hardware token to satisfy the requirement for advanced authentication. Once the detective's credentials are validated, his identity is asserted by the infrastructure to all authorized applications needed to complete his queries.

Use Case 2 – Use of a Smart Card

A user is issued a smart card that is loaded with user-specific digital certificates from a terminal within a controlled area. The user selects an application that will provide access to Criminal Justice Information (CJI) then enters the proper username (identification) and password ("something you know"). Once prompted, the user connects the smart card ("something you have") to the terminal. The user is prompted to enter a personal identification number (PIN) to unlock the smart card. Once unlocked, the smart card sends the certificates to the authentication management server at the local agency where the combined username, password, and digital user certificates are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 3 – Out of Band One-Time-Password (OTP) – Mobile phone-based

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password ("something you know"). Once that has been completed, a text message containing a one-time password (OTP) is sent via text message (out of band) to the user's agency-issued cell phone. The user is challenged via the CJI application for that OTP. The user enters the OTP ("something you have") then the username, password, and OTP are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 4 – Improper Use of a One-Time-Password (OTP) – Laptop

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password ("something you know"). Once that has been completed, a one-time password (OTP) is sent to the user's agency-issued laptop (in band) via pop-up message. The user is challenged via the CJI application for that OTP; however, the delivery of the OTP to the device that is being used to access CJI (in band) defeats the purpose of the second factor. This method does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI. See the below explanation:

This method of receiving the necessary OTP (in band) does not guarantee the authenticity of the user's identity because anyone launching the CJI application and entering a valid username/password combination is presented the OTP via a pop-up which is intend to be the second factor of authentication. This method makes the application accessible to anyone with knowledge of the valid username and password. Potentially, this is no more secure than using only a single factor of authentication.

Use Case 5 – Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires email access (containing Criminal Justice Information) via an Outlook Web Access (OWA) client utilizes a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password ("something you know"). The RBA detects this computer has not previously been used by the user, is not listed under the user's profile, and then presents high-risk challenge/response question(s) which the user is prompted to answer. Once the questions have been verified as correct, the user is authenticated and granted access to the email. Meanwhile, the RBA logs and collects a number of device forensic information and captures the user pattern analysis to update the user's profile. The CJIS Security Policy requirements for RBA have been satisfied.

Use Case 6 – Improper Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires access to email containing Criminal Justice Information (CJI) via an Outlook Web Access (OWA) client utilizing a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password ("something you know"). The RBA detects this computer has not previously been used by the user and is not listed under the user's profile. The user is prompted to answer high-risk challenge/response questions for verification and authorization to access to the email; however, if the second authentication factor is to answer additional questions presented every time the user logs on, then this solution is referred to as a knowledge-based authentic on (KBA) solution. A KBA solution does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI.

See the below explanation:

A KBA solution is not a viable advanced authentication (AA) solution per the CJIS Security Policy (CSP). The KBA asks questions and compares the answers to those stored within the user's profile. A KBA is neither a CSP compliant two factor authentication solution, nor does it meet the CSP criteria of a risk-based authentication (RBA) solution which logs and collects a number of device forensic information and captures the user pattern analysis to update the user's profile. Using this collected data, the RBA presents challenge/response questions when changes to the user's profile are noted versus every time the user logs in.

Use Case 7 – Advanced Authentication Compensating Controls on Agency-Issued Smartphones

An authorized user is issued a smartphone that is administratively managed by the agency-installed mobile device management (MDM) solution to ensure device compliance with the CJIS Security Policy. The user initiates an email client on the smartphone that contains emails with CJI. The email client challenges the user to enter a username (identification) and a password (one factor: something you know) which are forwarded to the local agency for authentication. The smartphone lacks the technical capability to challenge the user for a second factor of authentication. This email client is used across the state agency so access is a necessity for the user's job functions.

An audit by the CSA identifies the agency's use of the agency smartphone as not compliant with AA requirements due to the authorized user authenticating with only one factor instead of the required two factors.

Subsequently, the agency performs a risk assessment of their smartphone authentication solution and document a legitimate technical constraint due to the lack of technical solutions for smartphone-based two-factor authentication. The risk assessment identifies the following compensating controls that, when combined with the authorized user authenticating to the local agency with their password, meet the intent of the AA requirement by providing a similar level of security:

1. Enhance smartphone policy to enable possession of the smartphone to be considered a factor of authentication (i.e. something you have). Require authorized users to treat the smartphone as a controlled device and protect it as they would a personal credit card or an issued firearm to ensure only they will be in possession of the device

2. Move the email client used to authenticate with the local agency inside an encrypted, password-protected secure container on the smartphone ensuring only the authorized user can access the email application to authenticate.

The agency submits an AA compensating controls request to the CSO outlining the technical constraint identified by the risk assessment, what compensating controls will be employed, and the desired duration of the compensating controls.

The CSO approves the agency's request and provides documentation of the approval to the agency to maintain for audit purposes. The agency enacts the compensating controls and informs agency personnel they are permitted to access CJI via the agency-issued smartphone.

Figure 9 – Authentication Decision for Known Location

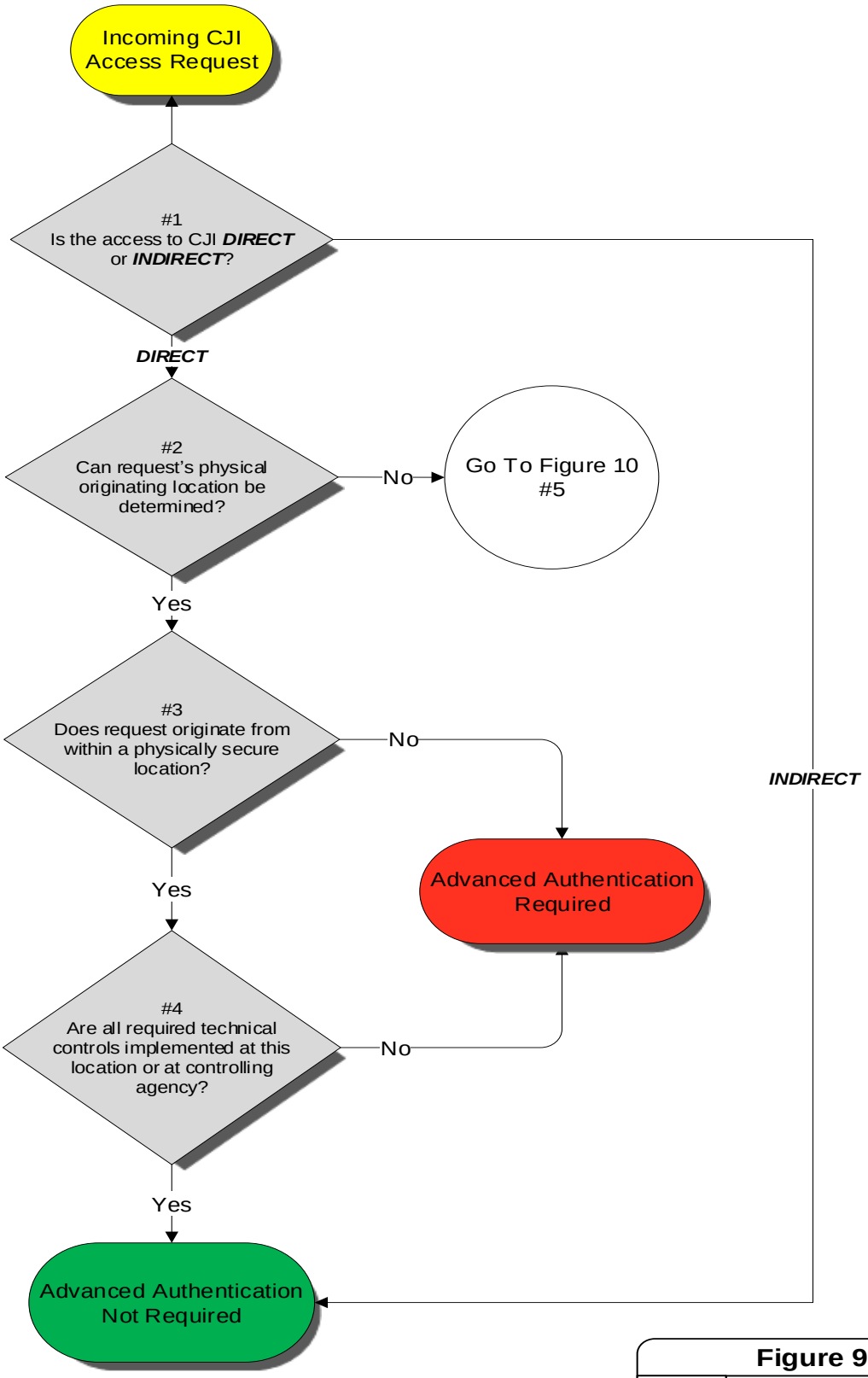


Figure 9
06/01/2020

Figure 10 – Authentication Decision for Unknown Location

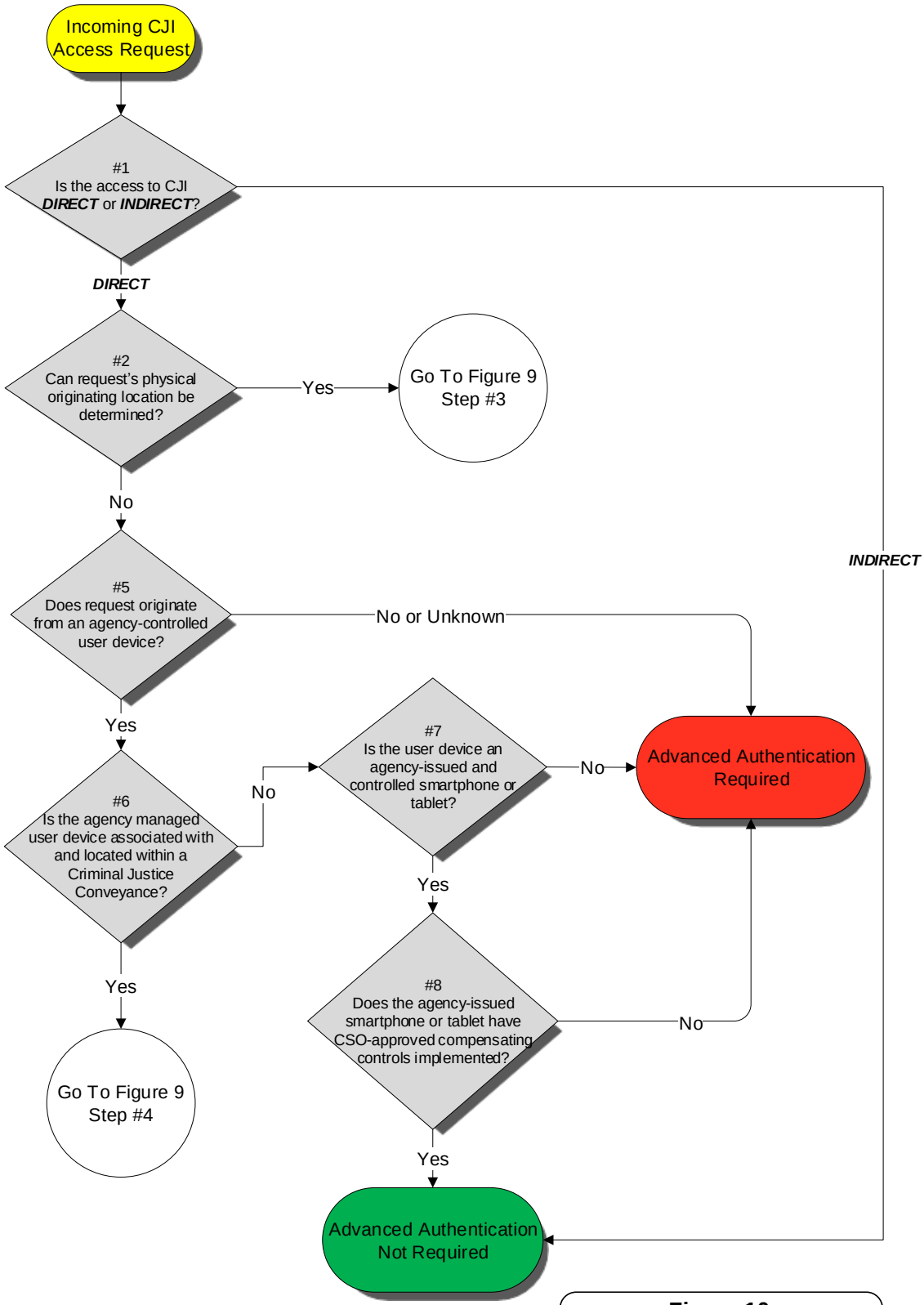


Figure 10
06/01/2020

5.7 Policy Area 7: Configuration Management

5.7.1 Access Restrictions for Changes

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. Section 5.5, Access Control, describes agency requirements for control of privileges and restrictions.

5.7.1.1 Least Functionality

The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

5.7.1.2 Network Diagram

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams.

The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. "For Official Use Only" (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.

5.7.2 Security of Configuration Documentation

The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

Figure 11 – A Local Police Department's Configuration Management Controls

A local police department decided to update their CAD system, and in doing so tracked all changes made to their infrastructure in a configuration management journal, updated their network topology documents to include all new components in their architecture, then marked all documentation as FOUO and stored them securely.

5.8 Policy Area 8: Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

5.8.1 Media Storage and Access

The agency shall securely store digital and physical media within physically secure locations or controlled areas. The agency shall restrict access to digital and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

5.8.2 Media Transport

The agency shall protect and control digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

5.8.2.1 Digital Media during Transport

Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data.

5.8.2.2 Physical Media in Transit

The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

5.8.3 Digital Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

Figure 12 – A Local Police Department's Media Management Policies

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. The police department contracted with an off-site media manager to store backups of their data in the contractor's vaults, but the contractor was not authorized to process or store CJI. To ensure the confidentially of the police department's data while outside its perimeter, they encrypted all data going to the contractor with an encryption product that is FIPS 140-2 certified. The police department rotated and reused media through the contractor's vaults periodically, and when it required destruction, the police department incinerated the media to irreversibly destroy any data on it.

5.9 Policy Area 9: Physical Protection

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

5.9.1 Physically Secure Location

A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof.

Sections 5.9.1.1 – 5.9.1.8 describe the physical controls required in order to be considered a physically secure location, while Sections 5.2 and 5.12, respectively, describe the minimum security awareness training and personnel security controls required for unescorted access to a physically secure location. Sections 5.5, 5.6.2.2.1, and 5.10 describe the requirements for technical security controls required to access CJI from within the perimeter of a physically secure location without AA.

5.9.1.1 Security Perimeter

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.

5.9.1.2 Physical Access Authorizations

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

5.9.1.3 Physical Access Control

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

5.9.1.4 Access Control for Transmission Medium

The agency shall control physical access to information system distribution and transmission lines within the physically secure location.

5.9.1.5 Access Control for Display Medium

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

5.9.1.6 Monitoring Physical Access

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

5.9.1.7 Visitor Control

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.

5.9.1.8 Delivery and Removal

The agency shall authorize and control information system-related items entering and exiting the physically secure location.

5.9.2 Controlled Area

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
2. Lock the area, room, or storage container when unattended.
3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
4. Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e. data "at rest") of CJI.

Figure 13 – A Local Police Department's Physical Protection Measures

A local police department implemented a replacement CAD system that was authorized to process CJI over an encrypted VPN tunnel to the state's CSA. The police department established a physically separated wing within their precinct separated by locked doors, walls, and a monitored security system within which CJI was processed by criminal justice professionals. Only those persons with the appropriate authorizations were permitted within this wing unless accompanied by such a person. Within this secure wing the police department further segregated the back-office information systems' infrastructure within a separately controlled area restricted only to those authorized administrative personnel with a need to enter.

5.10 Policy Area 10: System and Communications Protection and Information Integrity

Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the policy for protecting systems and communications infrastructures.

Refer to Section 5.13.4 for additional system integrity requirements related to mobile devices used to access CJI.

5.10.1 Information Flow Enforcement

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are:

1. Prevent CJI from being transmitted unencrypted across the public network.
2. Block outside traffic that claims to be from within the agency.
3. Do not pass any web requests to the public network that are not from the internal web proxy.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

5.10.1.1 Boundary Protection

The agency shall:

1. Control access to networks processing CJI.
2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.13.4.3 for guidance on personal firewalls.
4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device "fails closed" vs. "fails open").

6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in Section 5.10.3.2 to achieve separation.

5.10.1.2 Encryption

Encryption is a form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information. Decryption is the reversing of the cryptographic operation to convert the information back into a plaintext (readable) format. There are two main types of encryption: symmetric encryption and asymmetric encryption (also known as public key encryption). Hybrid encryption solutions do exist and use both asymmetric encryption for client/server certificate exchange – session integrity and symmetric encryption for bulk data encryption – data confidentiality.

5.10.1.2.1 Encryption for CJI in Transit

When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.

NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

EXCEPTIONS:

1. See Sections 5.13.1.2.2 and 5.10.2.
2. Encryption shall not be required if the transmission medium meets all of the following requirements:
    a. The agency owns, operates, manages, or protects the medium.
    b. Medium terminates within physically secure locations at both ends with no interconnections between.
    c. Physical access to the medium is controlled by the agency using the requirements in Sections 5.9.1 and 5.12.
    d. Protection includes safeguards (e.g., acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g., alarms, notifications) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.
    e. With prior approval of the CSO.

Examples:

- A campus is completely owned and controlled by a criminal justice agency (CJA) – If line-of-sight between buildings exists where a cable is buried, encryption is not required.

- A multi-story building is completely owned and controlled by a CJA – If floors are physically secure or cable runs through non-secure areas are protected, encryption is not required.
- A multi-story building is occupied by a mix of CJAs and non-CJAs – If floors are physically secure or cable runs through the non-secure areas are protected, encryption is not required.

5.10.1.2.2 Encryption for CJI at Rest

When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

1. When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:
    a. Be at least 10 characters
    b. Not be a dictionary word.
    c. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
    d. Be changed when previously authorized personnel no longer require access.
2. Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.

    NOTE: Commonly available encryption tools often use a key to unlock the cipher to allow data access; this key is called a passphrase. While similar to a password, a passphrase is not used for user authentication. Additionally, the passphrase contains stringent character requirements making it more secure and thus providing a higher level of confidence that the passphrase will not be compromised.

5.10.1.2.3 Public Key Infrastructure (PKI) Technology

For agencies using public key infrastructure (PKI) technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:

1. Include authorization by a supervisor or a responsible official.
2. Be accomplished by a secure process that verifies the identity of the certificate holder.
3. Ensure the certificate is issued to the intended party.

5.10.1.3 Intrusion Detection Tools and Techniques

Intrusion detection systems are deployed inside a network to monitor events against a known set of parameters (i.e. malicious activity or policy violations) and make notification to the system of any event which violates any of those parameters. They are passive in nature, listening and

monitoring network traffic. There are mainly two types of IDS; network-based IDS (NIDS) and host-based IDS (HIDS).

Intrusion prevention systems are an IDS with the capability to respond to detected intrusions. They are normally deployed at the perimeter of a network, scanning traffic. Like detection systems, protection systems compare scanned traffic to defined normal parameters but unlike detection systems are able to take some type of immediate action to mitigate, or prevent, an event.

Agencies shall:

1. Implement network-based and/or host-based intrusion detection or prevention tools.
2. Maintain current intrusion detection or prevention signatures.
3. Monitor inbound and outbound communications for unusual or unauthorized activities.
4. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
5. Review intrusion detection or prevention logs weekly or implement automated event notification.
6. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

5.10.1.4 Voice over Internet Protocol

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are lower costs than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol (IP) services. Among VoIP's risks that have to be considered carefully are: myriad security concerns, cost issues associated with new networking hardware requirements, and overarching quality of service (QoS) factors.

In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:

1. Establish usage restrictions and implementation guidance for VoIP technologies.
2. Change the default administrative password on the IP phones and VoIP switches.
3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.

Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.

5.10.1.5 Cloud Computing

Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, NIST Special Publications (800-144, 800-

145, and 800-146), as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e. U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).

Note: This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange agreements (i.e. the Preventing and Combating Serious Crime (PCSC) agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).

Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

The agency may permit limited use of metadata derived from unencrypted CJI when specifically approved by the agency and its "intended use" is detailed within the service agreement. Such authorized uses of metadata may include, but are not limited to the following: spam and spyware filtering, data loss prevention, spillage reporting, transaction logs (events and content – similar to Section 5.4), data usage/indexing metrics, and diagnostic/syslog data.

5.10.2 Facsimile Transmission of CJI

CJI transmitted via a single or multi-function device over a standard telephone line is exempt from encryption requirements. CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, shall meet the encryption requirements for CJI in transit as defined in Section 5.10.

5.10.3 Partitioning and Virtualization

As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization have existed for a while, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.

5.10.3.1 Partitioning

The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.

The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:

1. Different computers.

2. Different central processing units.
3. Different instances of the operating system.
4. Different network addresses.
5. Other methods approved by the FBI CJIS ISO.

5.10.3.2 Virtualization

Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice activities. In addition to the security controls described in this Policy, the following additional controls shall be implemented in a virtual environment:

1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines (VMs) that process CJI internally or be separated by a virtual firewall.
4. Drivers that serve critical functions shall be stored within the specific VM they service. In other words, do not store these drivers within the hypervisor, or host operating system, for sharing. Each VM is to be treated as an independent system – secured as independently as possible.

The following additional technical security controls shall be applied in virtual environments where CJI is comingled with non-CJI:

1. Encrypt CJI when stored in a virtualized environment where CJI is comingled with non-CJI or segregate and store unencrypted CJI within its own secure VM.
2. Encrypt network traffic within the virtual environment.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Implement IDS and/or IPS monitoring within the virtual environment.
2. Virtually or physically firewall each VM within the virtual environment to ensure that only allowed protocols will transact.
3. Segregate the administrative duties for the host.

Appendix G-1 provides some reference and additional background information on virtualization.

5.10.4 System and Information Integrity Policy and Procedures

5.10.4.1 Patch Management

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as:

1. Testing of appropriate patches before installation.
2. Rollback capabilities when installing patches, updates, etc.
3. Automatic updates without individual user intervention.
4. Centralized patch management.

Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

5.10.4.2 Malicious Code Protection

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

5.10.4.3 Spam and Spyware Protection

The agency shall implement spam and spyware protection.

The agency shall:

1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
2. Employ spyware protection at workstations, servers and mobile computing devices on the network.
3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this Policy.

5.10.4.4 Security Alerts and Advisories

The agency shall:

1. Receive information system security alerts/advisories on a regular basis.
2. Issue alerts/advisories to appropriate personnel.
3. Document the types of actions to be taken in response to security alerts/advisories.
4. Take appropriate actions in response.

5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

5.10.4.5 Information Input Restrictions

The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only.

Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Figure 14 – System and Communications Protection and Information Integrity Use Cases

Use Case 1 – A Local Police Department's Information Systems & Communications Protections

A local police department implemented a replacement CAD system within a physically secure location that was authorized to process CJI using a FIPS 140-2 encrypted VPN tunnel over the Internet to the state's CSA. In addition to the policies, physical and personnel controls already in place, the police department employed firewalls both at their border and at key points within their network, intrusion detection systems, a patch-management strategy that included automatic patch updates where possible, virus scanners, spam and spyware detection mechanisms that update signatures automatically, and subscribed to various security alert mailing lists and addressed vulnerabilities raised through the alerts as needed.

Use Case 2 – Faxing from a Single/Multi-function Device over a Traditional Telephone Line

A dispatcher from county A runs a NCIC query on an individual. The results are printed and then sent to an adjoining county using a single/multi-function device with facsimile capability. For faxing, the device is only connected to a traditional telephone line as is the device at the receiving county. Encryption of a document containing CJI is not required because the document travels over a traditional telephone line.

Use Case 3 – Faxing from a Multi-function Device over a Network

A dispatcher from city A runs a NCIC query on an individual. The results are printed and the dispatcher uses a multi-function copier to fax the file to a city in another state. The dispatcher enters the fax number of the receiver and sends the document. The document containing CJI is automatically converted to a digital file and routed to the receiver over the agency network and the Internet. Because the device uses a network and the Internet for transmitting documents containing CJI, encryption in transit using FIPS 140-2 certified 128 bit symmetric encryption is required.

5.11 Policy Area 11: Formal Audits

Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies.

5.11.1 Audits by the FBI CJIS Division

5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

5.11.1.2 Triennial Security Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.

5.11.2 Audits by the CSA

Each CSA shall:

1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.
3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
4. Have the authority, on behalf of another CSA, to conduct a CSP compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.

Note: This authority does not apply to the audit requirement outlined in the Security and Management Control Outsourcing Standard for Non-Channeler and Channelers related to outsourcing noncriminal justice administrative functions.

5.11.3 Special Security Inquiries and Audits

All agencies having access to CJI shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.

5.11.4 Compliance Subcommittees

The Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) established the Compliance Evaluation Subcommittee (CES) to evaluate the results of audits conducted by the CJIS Audit Unit (CAU). The CES makes specific recommendations to the APB concerning compliance with applicable policies and regulations. The most current information regarding the CAU audits that are within the purview of the CES and detailed CES sanctions process procedures are available at CJIS.gov (Law Enforcement Enterprise Portal) CJIS Special Interest Groups CES Section and CJIS Section of FBI.gov.

The National Crime Prevention and Privacy Compact (Compact) Council at Article VI established the Compact Council (Council). The Compact Council Sanctions Committee is responsible for ensuring the use of the Interstate Identification Index System for noncriminal justice purposes complies with the Compact and with rules, standards, and procedures established by the Compact Council. As such, the Sanctions Committee reviews the results of audits conducted by the Federal Bureau of Investigation (FBI) of participants in the FBI's Criminal Justice Services (CJIS) Division programs. The Sanctions Committee reviews the audit results and the participant's response to determine a course of action necessary to bring the participant into compliance and make recommendations to the Compact Council or the FBI. Additional information on the Compact Council Sanctions process is available on the Compact Council's web-site.

Figure 15 – The Audit of a Local Police Department

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. Shortly after the implementation, their state's CSA conducted an audit of their policies, procedures, and systems that process CJI. The police department supplied all architectural and policy documentation, including detailed network diagrams, to the auditors in order to assist them in the evaluation. The auditors discovered a deficiency in the police department's systems and marked them "out" in this aspect of the FBI CJIS Security Policy. The police department quickly addressed the deficiency and took corrective action, notifying the auditors of their actions.

5.12 Policy Area 12: Personnel Security

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have unescorted access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI

1. To verify identification, state of residency and national fingerprint-based record checks shall be conducted prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing). However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:

    a. 5 CFR 731.106; and/or

    b. Office of Personnel Management policy, regulations, and guidance; and/or

    c. agency policy, regulations, and guidance.

    Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

    See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.

2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.

3. If a record of any kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.

    a. If a felony conviction of any kind exists, the Interface Agency shall deny access to CJI. However, the Interface Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

    b. Applicants with a record of misdemeanor offense(s) may be granted access if the CSO, or his or her designee, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The Interface Agency may request the CSO review a denial of access determination. This same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.

    c. If a record of any kind is found on a contractor, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the contractor's security officer.

4. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
5. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.
6. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
7. The granting agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

5.12.2 Personnel Termination

Upon termination of personnel by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI. Furthermore, the interface agency shall provide notification or other action to ensure access to state and other agency systems is terminated. If the employee is an employee of a NCJA or a Contractor, the employer shall notify all Interface Agencies that may be affected by the personnel change.

5.12.3 Personnel Transfer

The agency shall review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.

5.12.4 Personnel Sanctions

The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Figure 16 – A Local Police Department's Personnel Security Controls

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. In addition to the physical and technical controls already in place, the police department implemented a variety of personnel security controls to reduce the insider threat. The police department used background screening consistent with the FBI CJIS Security Policy to vet those with unescorted access to areas in which CJI is processed, including the IT administrators employed by a contractor and all janitorial staff. The police department established sanctions against any vetted person found to be in violation of stated

policies. The police department re-evaluated each person's suitability for access to CJI every five years.

5.13 Policy Area 13: Mobile Devices

This policy area describes considerations and requirements for mobile devices including smartphones and tablets. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section augment those in other areas of the Policy to address the gaps introduced by using mobile devices.

The agency shall: (i) establish usage restrictions and implementation guidance for mobile devices; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.

Appendix G provides reference material and additional information on mobile devices.

5.13.1 Wireless Communications Technologies

Examples of wireless communication technologies include, but are not limited to: 802.11, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls as described below.

5.13.1.1 802.11 Wireless Protocols

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.

Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
5. Enable user authentication and encryption mechanisms for the management interface of the AP.
6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Section 5.6.2.1.
7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.

8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.
10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
11. Ensure that the ad hoc mode has been disabled.
12. Disable all nonessential management protocols on the APs.
13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.
14. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
15. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

5.13.1.2 Cellular Devices

Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), tablets, personal digital assistants (PDA), and "aircards" are examples of cellular handheld devices or devices that are capable of employing cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks.

Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

1. Loss, theft, or disposal.
2. Unauthorized access.
3. Malware.
4. Spam.
5. Electronic eavesdropping.
6. Electronic tracking (threat to security of data and safety of the criminal justice professional).
7. Cloning (not as prevalent with later generation cellular technologies).
8. Server-resident data.

5.13.1.2.1 Cellular Service Abroad

Certain internal functions on cellular devices may be modified or compromised by the cellular carrier during international use as the devices are intended to have certain parameters configured by the cellular provider which is considered a "trusted" entity by the device.

When devices are authorized to access CJI outside the U.S., agencies shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency's policies prior to and after deployment outside of the U.S.

5.13.1.2.2 Voice Transmissions Over Cellular Devices

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements.

5.13.1.3 Bluetooth

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth is used primarily to establish wireless personal area networks (WPAN). Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices.

Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g. denial of service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation) as well as specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency's operational and business processes.

5.13.1.4 Mobile Hotspots

Many mobile devices include the capability to function as a WiFi hotspot that allows other devices to connect through the device to the internet over the devices cellular network.

When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured:

1. Enable encryption on the hotspot
2. Change the hotspot's default SSID
    a. Ensure the hotspot SSID does not identify the device make/model or agency ownership
3. Create a wireless network password (Pre-shared key)
4. Enable the hotspot's port filtering/blocking features if present
5. Only allow connections from agency controlled devices

Note: Refer to the requirements in Section 5.10.1.2 encryption for item #1. Refer to the requirements in Section 5.6.2.2.1 Password for item #3. Only password attributes #1, #2 and #3 are required.

OR

1. Have a MDM solution to provide the same security as identified in items 1 – 5 above.

5.13.2 Mobile Device Management (MDM)

Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery, if so desired by the agency.

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of full-featured operating systems may not function properly on devices with limited-feature operating systems. MDM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented.

Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time. User agencies shall implement the following controls when directly accessing CJI from devices running a limited-feature operating system:

1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration configured and implemented to perform at least the following controls:
    a. Remote locking of device
    b. Remote wiping of device
    c. Setting and locking device configuration
    d. Detection of "rooted" and "jailbroken" devices
    e. Enforcement of folder or disk level encryption
    f. Application of mandatory policy settings on the device
    g. Detection of unauthorized configurations
    h. Detection of unauthorized software or applications
    i. Ability to determine the location of agency controlled devices
    j. Prevention of unpatched devices from accessing CJI or CJI systems
    k. Automatic device wiping after a specified number of failed access attempts

EXCEPTION: An MDM is not required when receiving CJI from an indirect access information system (i.e. the system provides no capability to conduct transactional activities on state and national repositories, applications or services). However, it is incumbent upon the authorized agency to ensure CJI is delivered to the appropriate requesting agency or individual. The CSO will make the final determination of whether access is considered indirect.

5.13.3 Wireless Device Risk Mitigations

Organizations shall, at a minimum, ensure that wireless devices:

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.

2. Are configured for local device authentication (see Section 5.13.7.1).
3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.
4. Encrypt all CJI resident on the device.
5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.
6. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.

5.13.4 System Integrity

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full-featured operating systems. In many cases, the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM, application, or supporting service infrastructure.

5.13.4.1 Patching/Updates

Based on the varying connection methods for mobile devices, an always on connection cannot be guaranteed for patching and updating. Devices without always-on cellular connections may not be reachable for extended periods of time by the MDM or solution either to report status or initiate patching.

Agencies shall monitor mobile devices to ensure their patch and update state is current.

5.13.4.2 Malicious Code Protection

Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software and can provide a high degree of confidence that only known software or applications are installed on the device.

Agencies that allow smartphones and tablets to access CJI shall have a process to approve the use of specific software or applications on the devices. Any device natively capable of performing these functions without a MDM solution is acceptable under this section.

5.13.4.3 Personal Firewall

For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

1. Manage program access to the Internet.

2. Block unsolicited requests to connect to the user device.
3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

Mobile devices with limited-feature operating systems (i.e. tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform functions similar to a personal firewall on a device with a full-feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.

5.13.5 Incident Response

In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.

Special reporting procedures for mobile devices shall apply in any of the following situations:

1. Loss of device control. For example:
    a. Device known to be locked, minimal duration of loss
    b. Device lock state unknown, minimal duration of loss
    c. Device lock state unknown, extended duration of loss
    d. Device known to be unlocked, more than momentary duration of loss
2. Total loss of device
3. Device compromise
4. Device loss or compromise outside the United States

5.13.6 Access Control

Multiple user accounts are not generally supported on limited-feature mobile operating systems. Access control (Section 5.5 Access Control) shall be accomplished by the application that accesses CJI.

5.13.7 Identification and Authentication

Due to the technical methods used for identification and authentication on many limited-feature mobile operating systems, achieving compliance may require many different components.

5.13.7.1 Local Device Authentication

When mobile devices are authorized for use in accessing CJI, local device authentication shall be used to unlock the device for use. The authenticator used shall meet the requirements in section 5.6.2.1 Standard Authenticators.

5.13.7.2 Advanced Authentication

When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user unless the access to CJI is indirect as described in Section 5.6.2.2.1. If access is indirect, then AA is not required.

5.13.7.2.1 Compensating Controls

CSO approved compensating controls to meet the AA requirement on agency-issued smartphones and tablets with limited-feature operating systems are permitted. Compensating controls are temporary control measures that are implemented in lieu of the required AA control measures when an agency cannot meet a requirement due to legitimate technical or business constraints. Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.13.2. The compensating controls shall:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls
4. Expire upon the CSO approved date or when a compliant AA solution is implemented.

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

The compensating controls for AA are a combination of controls providing acceptable assurance only the authorized user is authenticating and not an impersonator or (in the case of agency-issued device used by multiple users) controls that reduce the risk of exposure if information is accessed by an unauthorized party.

The following minimum controls shall be implemented as part of the CSO approved compensating controls:

- Possession and registration of an agency issued smartphone or tablet as an indication it is the authorized user
- Use of device certificates per Section 5.13.7.3 Device Certificates
- Implemented CJIS Security Policy compliant standard authenticator protection on the secure location where CJI is stored

5.13.7.3 Device Certificates

Device certificates are often used to uniquely identify mobile devices using part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of device identification or authentication in a larger scheme, a device certificate alone placed on the device shall not be considered valid proof that the device is being operated by an authorized user.

When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they shall be:

1. Protected against being extracted from the device
2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts
3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use

APPENDICES

APPENDIX A TERMS AND DEFINITIONS

Access to Criminal Justice Information — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Administration of Criminal Justice — The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes "crime prevention programs" to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in Neighborhood Watch or "safe house" programs) and the result of such checks will not be disseminated outside the law enforcement agency.

Agency Controlled Mobile Device — A mobile device that is centrally managed by an agency for the purpose of securing the device for potential access to CJI. The device can be agency issued or BYOD (personally owned).

Agency Coordinator (AC) — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and agency.

Agency Issued Mobile Device — A mobile device that is owned by an agency and issued to an individual for use. It is centrally managed by the agency for the purpose of securing the device for potential access to CJI. The device is not BYOD (personally owned).

Agency Liaison (AL) — Coordinator of activities between the criminal justice agency and the noncriminal justice agency when responsibility for a criminal justice system has been delegated by a criminal justice agency to a noncriminal justice agency, which has in turn entered into an agreement with a contractor. The agency liaison shall, inter alia, monitor compliance with system security requirements. In instances in which the noncriminal justice agency's authority is directly from the CJIS systems agency, there is no requirement for the appointment of an agency liaison.

Asymmetric Encryption — A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Authorized User/Personnel — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Authorized Recipient — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

Availability — The degree to which information, a system, subsystem, or equipment is operable and in a useable state; frequently represented as a proportion of time the element is in a functioning condition.

Biographic Data — Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.

Biometric Data — When applied to CJI, it is used to identify individuals, and includes the following types: fingerprints, palm prints, DNA, iris, and facial recognition.

Case / Incident History — All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regards to CJI, it is the information about the history of criminal incidents.

Certificate Authority (CA) Certificate – Digital certificates required for certificate-based authentication that are issued to tell the client computers and servers that it can trust other certificates that are issued by this CA.

Channeler — A FBI approved contractor, who has entered into an agreement with an Authorized Recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees. The Channeler ensures fingerprint submissions are properly and adequately completed, electronically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to Authorized Recipients. A Channeler is essentially an "expediter" rather than a user of criminal history record check results.

Cloud Client – A machine or software application that accesses cloud services over a network connection, perhaps on behalf of a subscriber.

Cloud Computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services), software, and information.

Cloud Provider – An organization that provides cloud computing services.

Cloud Subscriber – A person or organization that is a customer of a cloud computing service provider.

CJIS Advisory Policy Board (APB) — The governing organization within the FBI CJIS Advisory Process composed of representatives from criminal justice and national security agencies within the United States. The APB reviews policy, technical, and operational issues relative to CJIS Division programs and makes subsequent recommendations to the Director of the FBI.

CJIS Audit Unit (CAU) — The organization within the FBI CJIS Division responsible to perform audits of CSAs to verify compliance with the CJIS Security Policy**.**

CJIS Security Policy — The FBI CJIS Security Policy document as published by the FBI CJIS ISO; the document containing this glossary.

CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJI from various systems managed by the FBI CJIS

Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

CJIS Systems Agency Information Security Officer (CSA ISO) — The appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies.

CJIS Systems Officer (CSO) — The individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf of the CJIS Systems Agency.

Compact Council — The entity created by the National Crime Prevention and Privacy Compact of 1998 that has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

Compact Officers — The leadership of the Compact Council, oversees the infrastructure established by the National Crime Prevention and Privacy Compact Act of 1998, which is used by ratifying states to exchange criminal records for noncriminal justice purposes. Their primary responsibilities are to promulgate rules and procedures for the effective and appropriate use of the III system.

Compensating Controls — Compensating controls are temporary control measures implemented in lieu of the required control measures when an agency cannot meet the AA requirement due to legitimate technical or business constraints. The compensating controls must:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

Computer Security Incident Response Capability (CSIRC) — A collection of personnel, systems, and processes that are used to efficiently and quickly manage a centralized response to any sort of computer security incident which may occur.

Confidentiality — The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Contractor — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

Contracting Government Agency (CGA) — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.

Crime Reports Data — The data collected through the Uniform Crime Reporting program and reported upon annually by the FBI CJIS division used to analyze the crime statistics for the United States.

Criminal History Record Information (CHRI) — A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Agency (CJA) — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Criminal Justice Agency User Agreement — A terms-of-service agreement that must be signed prior to accessing CJI. This agreement is required by each CJA and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.

Criminal Justice Conveyance — A criminal justice conveyance is any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods, with the requirements of Section 5.9.1.3.

Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

Criminal Justice Information Services Division (FBI CJIS or CJIS) — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Data — See Information and CJI.

Decryption – The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Degauss — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g. solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.

Department of Justice (DoJ) — The Department within the U.S. Government responsible to enforce the law and defend the interests of the United States according to the law, to ensure public safety against threats foreign and domestic, to provide federal leadership in preventing and controlling crime, to seek just punishment for those guilty of unlawful behavior, and to ensure fair and impartial administration of justice for all Americans.

Digital Media – Any form of electronic media designed to store data in a digital format. This includes, but is not limited to: memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Digital Signature – A digital signature consists of three algorithms: (1) A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. (2) A signing algorithm that, given a message and a private key, produces a signature. (3) A signature verifying algorithm that, given a message, public key, and a signature, either accepts or rejects the message's claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

Direct Access — (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Dissemination — The transmission/distribution of CJI to Authorized Recipients within an agency.

Encryption – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Escort – Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

Facsimile (Fax) – Facsimile is: (a) a document received and printed on a single or multi-function stand-alone device, (b) a single or multi-function stand-alone device for the express purpose of transmitting and receiving documents from a like device over a standard telephone line, or (c) a facsimile server, application, service which implements email-like technology and transfers documents over a network.

Federal Bureau of Investigation (FBI) — The agency within the DOJ responsible to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

FBI CJIS Information Security Officer (FBI CJIS ISO) — The FBI personnel responsible for the maintenance and dissemination of the FBI CJIS Security Policy; the liaison between the FBI and the CSA's ISOs and other relevant security points-of-contact (POCs); the provider of technical guidance as to the intent and implementation of technical policy issues; the POC for computer incident notification which also disseminates security alerts to the CSOs and ISOs.

Federal Information Security Management Act (FISMA) — The Federal Information Security Management Act of 2002, a US Federal law that established information security standards for the protection of economic and national security interests of the United States. It requires each federal agency to develop, document, and implement an agency-wide program to provide information

security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

For Official Use Only (FOUO) — A caveat applied to unclassified sensitive information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA), 5 U.S.C 522. In general, information marked FOUO shall not be disclosed to anybody except Government (Federal, State, tribal, or local) employees or contractors with a need to know.

Full-feature Operating System — Full-feature operating systems are traditional operating systems used by a standard desktop computer (e.g. Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). These operating systems are generally open to user control and configuration and therefore require configuration management to properly secure, or "harden", these devices from malicious network based technical attacks (e.g. malware, spyware, hackers, etc.). These operating systems require traditional protection applications such as antivirus programs and personal firewalls.

Guest Operating System — An operating system that has emulated hardware presented to it by a host operating system. Also referred to as the virtual machine (VM).

Hashing — The process of applying a mathematical algorithm to data to produce an alphanumeric value (i.e. hash value) to be used as a representative of that data.

Hash Value — The term that refers to an alphanumeric value which represents the result of applying a cryptographic hash function to data.

Host Operating System — In the context of virtualization, the operating system that interfaces with the actual physical hardware and arbitrates between it and the guest operating systems. It is also referred to as a hypervisor.

Hybrid Encryption — A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Hypervisor — See Host Operating System.

Identity History Data — Textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

In-Band – The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is the same as the one used for login.

Indirect Access – Having the authority to access systems containing CJI without providing the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (e.g. CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).

Information — See data and CJI.

Information Exchange Agreement — An agreement that codifies the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty-of-care over the other party's information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which

establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards and guidance.

Information Security Officer (ISO) — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversees the governance of security operations, and establishes information security training and awareness programs. The ISO also usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

Information System — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

Integrated Automated Fingerprint Identification System (IAFIS) — The national fingerprint and criminal history system maintained by the FBI CJIS Division that provides the law enforcement community with automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

Integrity — The perceived consistency of expected outcomes, actions, values, and methods of an individual or organization. As it relates to data, it is the concept that data is preserved in a consistent and correct state for its intended use.

Interconnection Security Agreement (ISA) — An agreement much like an Information Exchange Agreement as mentioned above, but concentrating more on formalizing the technical and security requirements pertaining to some sort of interface between the parties' information systems.

Interface Agency — A legacy term used to describe agencies with direct connections to the CSA. This term is now used predominantly in a common way to describe any sub-agency of a CSA or SIB that leverages the CSA or SIB as a conduit to FBI CJIS information.

Internet Protocol (IP) — A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Interstate Identification Index (III) — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

Intrusion Detection — The process of monitoring the events occurring in an information system or network and analyzing them for signs of possible incidents.

Intrusion Detection System — Software which automates the intrusion detection process.

Intrusion Prevention — The process of monitoring events occurring in an information system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

Intrusion Prevention System — Software which has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

Jailbreak (Jailbroken) — The process of attaining privileged control (known as "root access") of a device running the Apple iOS operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Laptop Devices – Laptop devices are mobile devices with a full-featured operating system (e.g. Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). Laptops are typically intended for transport via vehicle mount or portfolio-sized carry case, but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones), or mobile devices that feature a limited-feature operating system (e.g. tablets).

Law Enforcement Enterprise Portal (LEEP) — A secure, Internet-based communications portal provided by the FBI CJIS Division for use by law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. Its primary purpose is to provide a platform on which various law enforcement agencies can collaborate on FOUO matters.

Limited-feature Operating System — Limited-feature operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers (e.g. Apple iOS, Android, Windows Mobile, Blackberry OS, etc.). There operating systems permit limited user control, but are inherently more resistant than a full-feature operating system to certain types of network based technical attacks due to the limited-feature sets. Devices using these operating systems are required to be managed by a mobile device management solution.

Logical Access – The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.

Logical Partitioning – When the host operating system, or hypervisor, allows multiple guest operating systems to share the same physical resources.

Local Agency Security Officer (LASO) — The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.

Management Control Agreement (MCA) — An agreement between parties that wish to share or pool resources that codifies precisely who has administrative control over, versus overall management and legal responsibility for, assets covered under the agreement. An MCA must ensure the CJA's authority remains with regard to all aspects of Section 3.2.2. The MCA usually results in the CJA having ultimate authority over the CJI supporting infrastructure administered by the NCJA.

Metadata — Structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is commonly referred to as data about data, information about information, or information describing the characteristics of data.

Mobile Device — Any portable device used to access CJI via a wireless connection (e.g. cellular, WiFi, Bluetooth, etc.).

Mobile Device Management (MDM) — Centralized administration and control of mobile devices specifically including, but not limited to, cellular phones, smart phones, and tablets. Management typically includes the ability to configure device settings and prevent a user from changing them, remotely locating a device in the event of theft or loss, and remotely locking or wiping a device. Management can also include over-the-air distribution of applications and updating installed applications.

Mobile (WiFi) Hotspot — A mobile (WiFi) hotspot is a zone or area associated with a mobile device (e.g. smartphone, air card) allowing wireless connectivity to the Internet typically through a cellular connection.

National Crime Information Center (NCIC) — An information system which stores CJI which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

National Instant Criminal Background Check System (NICS) — A system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by Federal Firearms Licensees (FFLs) to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.

National Institute of Standards and Technology (NIST) — Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic and national security.

Noncriminal Justice Agency (NCJA) — A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

NCJA (Government) — A Federal, state, local, or tribal governmental agency or any subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would be the central IT organization within a state government that administers equipment on behalf of a state law-enforcement agency.

NCJA (Private) — A private agency or subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a local bank.

NCJA (Public) — A public agency or sub-unit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a county school board which uses CHRI to assist in employee hiring decisions.

Noncriminal Justice Purpose — The uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Office of Management and Budget (OMB) — The agency within the Executive Branch of the Federal government responsible to oversee the preparation of the federal budget, to assist in the

supervision of other Executive Branch agencies, and to oversee and coordinate the Presidential Administration's procurement, financial management, information, and regulatory policies.

One-time Password — A disposable, single-use standard authenticator for access CJI. One-time passwords are: minimum of six (6) randomly generated characters, valid for a single session, and if not used, expire within a minimum of five (5) minutes after issuance.

Out-of-Band — The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is separate from that used for login.

Outsourcing — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.

Outsourcing Standard — National Crime Prevention and Privacy Compact Council's Outsourcing Standard. The Compact Council's uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes.

Partitioning – Managing guest operating system, or virtual machine, access to hardware so that each guest OS can access its own resources but cannot encroach on the other guest operating systems resources or any resources not allocated for virtualization use.

Password Verifier (Verifier) – An entity or process that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status.

Personal Firewall — An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.

Personally Identifiable Information (PII) — PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Physical Access – The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

Physical Media – Physical media refers to media in printed form. This definition includes, but is not limited to, printed documents, printed imagery, printed facsimile.

Physical Partitioning – When the host operating system, or hypervisor, assigns separate physical resources to each guest operating systems, or virtual machine.

Physically Secure Location — A facility, a criminal justice conveyance, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

Pocket/Handheld Mobile Device – Pocket/Handheld mobile devices (e.g. smartphones) are intended to be carried in a pocket or holster attached to the body and feature an operating system

with limited functionality (e.g., iOS, Android, BlackBerry, etc.). This definition does not include tablet and laptop devices.

Property Data — Information about vehicles and property associated with a crime.

Rap Back — A NGI service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.

Receive-Only Terminal (ROT) – A device that is configured to accept a limited type of data but is technically prohibited from forming or transmitting data, browsing or navigating internal or external networks, or otherwise performing outside the scope of receive only (e.g., a printer, dumb terminal, etc.).

Repository Manager, or Chief Administrator — The designated manager of the agency having oversight responsibility for a CSA's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the repository manager and CSO may be the same person.

Root (Rooting, Rooted) — The process of attaining privileged control (known as "root access") of a device running the Android operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Salting –The process of applying a non-secret value to data prior to applying a cryptographic process, such as hashing. This process changes the value to be hashed in a manner designed to ensure an attacker cannot reuse the results of computations for one instance.

Secondary Dissemination — The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.

Security Addendum (SA) — A uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Sensitive But Unclassified (SBU) — Designation of information in the United States federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information, Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. Some categories of SBU information have authority in statute or regulation (e.g. SSI, CII) while others, including FOUO, do not. As of May 9, 2008, the more appropriate terminology to use is Controlled Unclassified Information (CUI).

Server/Client Computer Certificate (device-based) – Digital certificates that are issued to servers or client computers or devices by a CA and used to prove device identity between server and/or client computer devices during the authentication process.

Service — The organized system of apparatus, appliances, personnel, etc, that supply some tangible benefit to the consumers of this service. In the context of CJI, this usually refers to one of the applications that can be used to process CJI.

Shredder — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the paper into long, thin strips but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.

Smartphone – See pocket/handheld mobile devices.

Social Engineering — The act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

Software Patch — A piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems. As such, patches should be installed in a test environment prior to being installed in a live, operational system. Patches often can be found in multiple locations but should be retrieved only from sources agreed upon through organizational policy.

State and Federal Agency User Agreement — A written agreement that each CSA or SIB Chief shall execute with the FBI CJIS Division stating their willingness to demonstrate conformance with the FBI CJIS Security Policy prior to the establishment of connectivity between organizations. This agreement includes the standards and sanctions governing use of CJIS systems, as well as verbiage to allow the FBI to periodically audit the CSA as well as to allow the FBI to penetration test its own network from the CSA's interfaces to it.

State Compact Officer — The representative of a state that is party to the National Crime Prevention and Privacy Compact, and is the chief administrator of the state's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

State Identification Bureau (SIB) — The state agency with the responsibility for the state's fingerprint identification services.

State Identification Bureau (SIB) Chief — The SIB Chief is the designated manager of state's SIB. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

State of Residency – A state of residency is the state in which an individual claims and can provide documented evidence as proof of being his/her permanent living domicile. CJIS Systems Officers have the latitude to determine what documentation constitutes acceptable proof of residency.

Symmetric Encryption — A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.

System — Refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections. In the context of CJI, this usually refers to

applications and all interconnecting infrastructure required to use those applications that process CJI.

Tablet Devices – Tablet devices are mobile devices with a limited-feature operating system (e.g. iOS, Android, Windows RT, etc.). Tablets typically consist of a touch screen without a permanently attached keyboard intended for transport via vehicle mount or portfolio-sized carry case but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones) or mobile devices with full-featured operating systems (e.g. laptops).

Terminal Agency Coordinator (TAC) — Serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

User Certificate (user-based) – Digital certificates that are unique and issued to individuals by a CA. Though not always required to do so, these specific certificates are often embedded on smart cards or other external devices as a means of distribution to specified users. This certificate is used when individuals need to prove their identity during the authentication process.

Virtual Escort – Authorized personnel who actively monitor a remote maintenance session on Criminal Justice Information (CJI)-processing systems. The escort must have the ability to end the session at any time deemed necessary to ensure the protection and integrity of CJI at all times.

Virtual Machine (VM) – See Guest Operating System

Virtualization — Refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation or emulation allowing multiple operating systems, or images, to run concurrently on the same hardware.

Voice over Internet Protocol (VoIP) — A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Wireless Access Point – A wireless access point is a device that logically connects a wireless client device to an organization's enterprise network which processes unencrypted CJI.

Wireless (WiFi) Hotspot – A wireless (WiFi) hotspot is a zone or area within a fixed location allowing wireless connectivity to the Internet typically through a wired connection. Hotspots are typically available in public areas such as airports, hotels and restaurants.

APPENDIX B ACRONYMS

Acronym	Term
AA	Advanced Authentication
AC	Agency Coordinator
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
APB	Advisory Policy Board
BD-ADDR	Bluetooth-Enabled Wireless Devices and Addresses
BYOD	Bring Your Own Device
CAD	Computer-Assisted Dispatch
CAU	CJIS Audit Unit
CFR	Code of Federal Regulations
CGA	Contracting Government Agency
CHRI	Criminal History Record Information
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
ConOps	Concept of Operations
CSA	CJIS Systems Agency
CSIRC	Computer Security Incident Response Capability
CSO	CJIS Systems Officer
DAA	Designated Approving Authority
DoJ	Department of Justice

DoJCERT	DoJ Computer Emergency Response Team
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HTTP	Hypertext Transfer Protocol
IAFIS	Integrated Automated Fingerprint Identification System
IDS	Intrusion Detection System
III	Interstate Identification Index
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
LASO	Local Agency Security Officer
LEEP	Law Enforcement Enterprise Portal
LMR	Land Mobile Radio
MAC	Media Access Control
MCA	Management Control Agreement
MDM	Mobile Device Management
MITM	Man-in-the-Middle

MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NCJA	Noncriminal Justice Agency
NICS	National Instant Criminal Background Check System
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
OTP	One-time Password
PBX	Private Branch Exchange
PCSC	Preventing and Combating Serious Crime
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point-of-Contact
PSTN	Public Switched Telephone Network
QA	Quality Assurance
QoS	Quality of Service
RCMP	Royal Canadian Mounted Police
RF	Radio Frequency
SA	Security Addendum
SCO	State Compact Officer
SIB	State Identification Bureau

SIG	Special Interest Group
SP	Special Publication
SPRC	Security Policy Resource Center
SSID	Service Set Identifier
TAC	Terminal Agency Coordinator
TLS	Transport Layer Security
UCN	Universal Control Number
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

APPENDIX C NETWORK TOPOLOGY DIAGRAMS

Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the "big picture" – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.

The following diagrams, labeled Appendix C.1-A through C.1-D, are examples for agencies to utilize during the development, maintenance, and update stages of their own network diagrams. By using these example drawings as a guideline, agencies can form the foundation for ensuring compliance with Section 5.7.1.2 of the CJIS Security Policy.

The purpose for including the following diagrams in this Policy is to aid agencies in their understanding of diagram expectations and should not be construed as a mandated method for network topologies. It should also be noted that agencies are not required to use the identical icons depicted in the example diagrams and should not construe any depiction of a particular vendor product as an endorsement of that product by the FBI CJIS Division.

Appendix C.1-A is a conceptual overview of the various types of agencies that can be involved in handling of CJI, and illustrates several ways in which these interconnections might occur. This diagram is not intended to demonstrate the level of detail required for any given agency's documentation, but it provides the reader with some additional context through which to digest the following diagrams. Take particular note of the types of network interfaces in use between agencies, in some cases dedicated circuits with encryption mechanisms, and in other cases VPNs over the Internet. This diagram attempts to show the level of diversity possible within the law enforcement community. These diagrams in no way constitute a standard for network engineering, but rather, for the expected quality of documentation.

The next three topology diagrams, C.1-B through C.1-D, depict conceptual agencies. For C.1-B through C.1-D, the details identifying specific "moving parts" in the diagrams by manufacturer and model are omitted, but it is expected that any agencies producing such documentation will provide diagrams with full manufacturer and model detail for each element of the diagram. Note that the quantities of clients should be documented in order to assist the auditor in understanding the scale of assets and information being protected.

Appendix C.1-B depicts a conceptual state law enforcement agency's network topology and demonstrates a number of common technologies that are in use throughout the law enforcement community (some of which are compulsory per CJIS policy, and some of which are optional) including Mobile Broadband cards, VPNs, Firewalls, Intrusion Detection Devices, VLANs, and so forth. Note that although most state agencies will likely have highly-available configurations, the example diagram shown omits these complexities and only shows the "major moving parts" for clarity but please note the Policy requires the logical location of all components be shown. The level of detail depicted should provide the reader with a pattern to model future documentation from, but should not be taken as network engineering guidance.

Appendix C.1-C depicts a conceptual county law enforcement agency. A number of common technologies are presented merely to reflect the diversity in the community, including proprietary

Packet-over-RF infrastructures and advanced authentication techniques, and to demonstrate the fact that agencies can act as proxies for other agencies.

Appendix C.1-D depicts a conceptual municipal law enforcement agency, presumably a small one that lacks any precinct-to-patrol data communications. This represents one of the smallest designs that could be assembled that, assuming all other details are properly considered, would meet the criteria for Section 5.7.1.2. This diagram helps to demonstrate the diversity in size that agencies handling criminal justice data exhibit.

Figure C-1-A Overview: Conceptual Connections Between Various Agencies

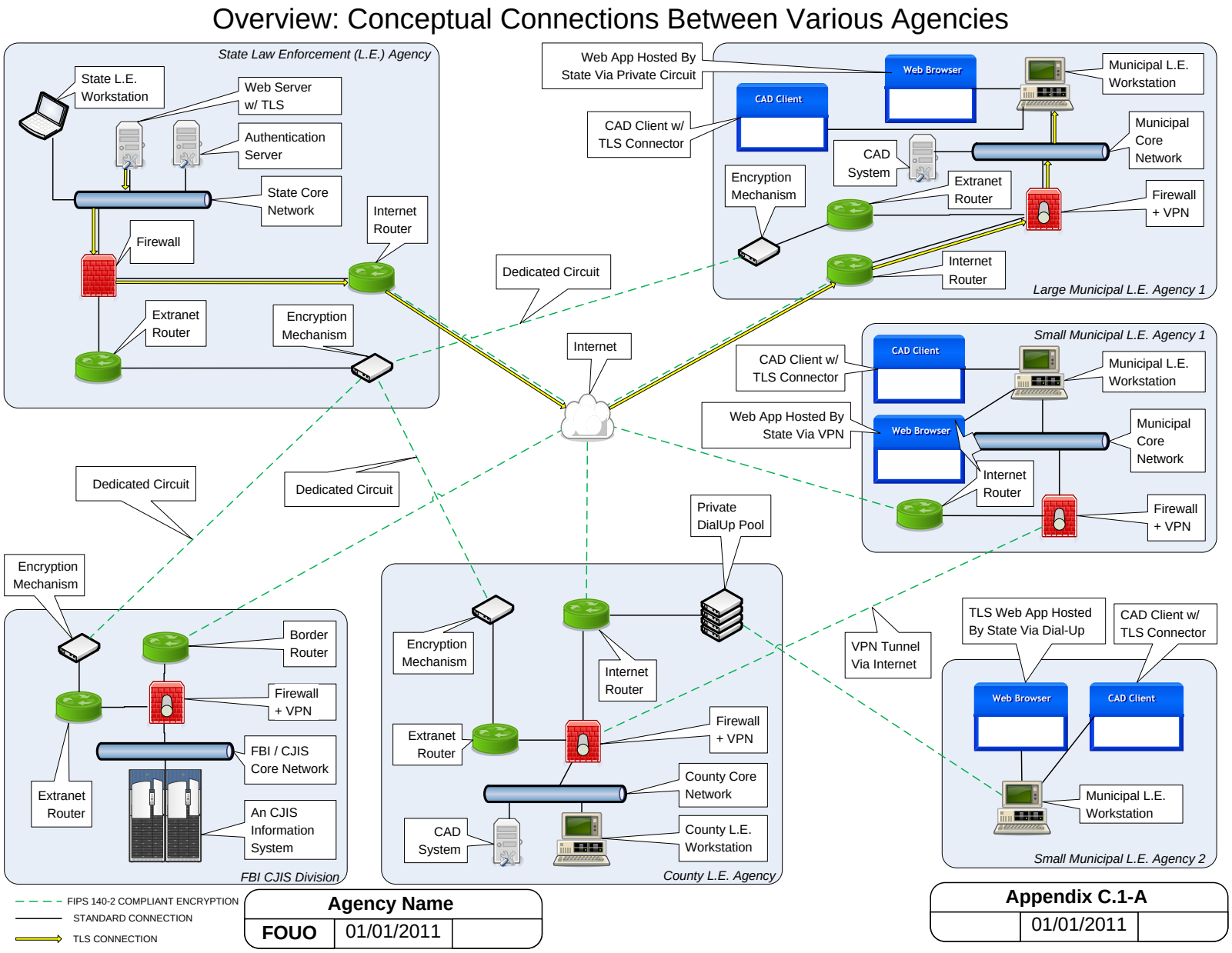


Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency

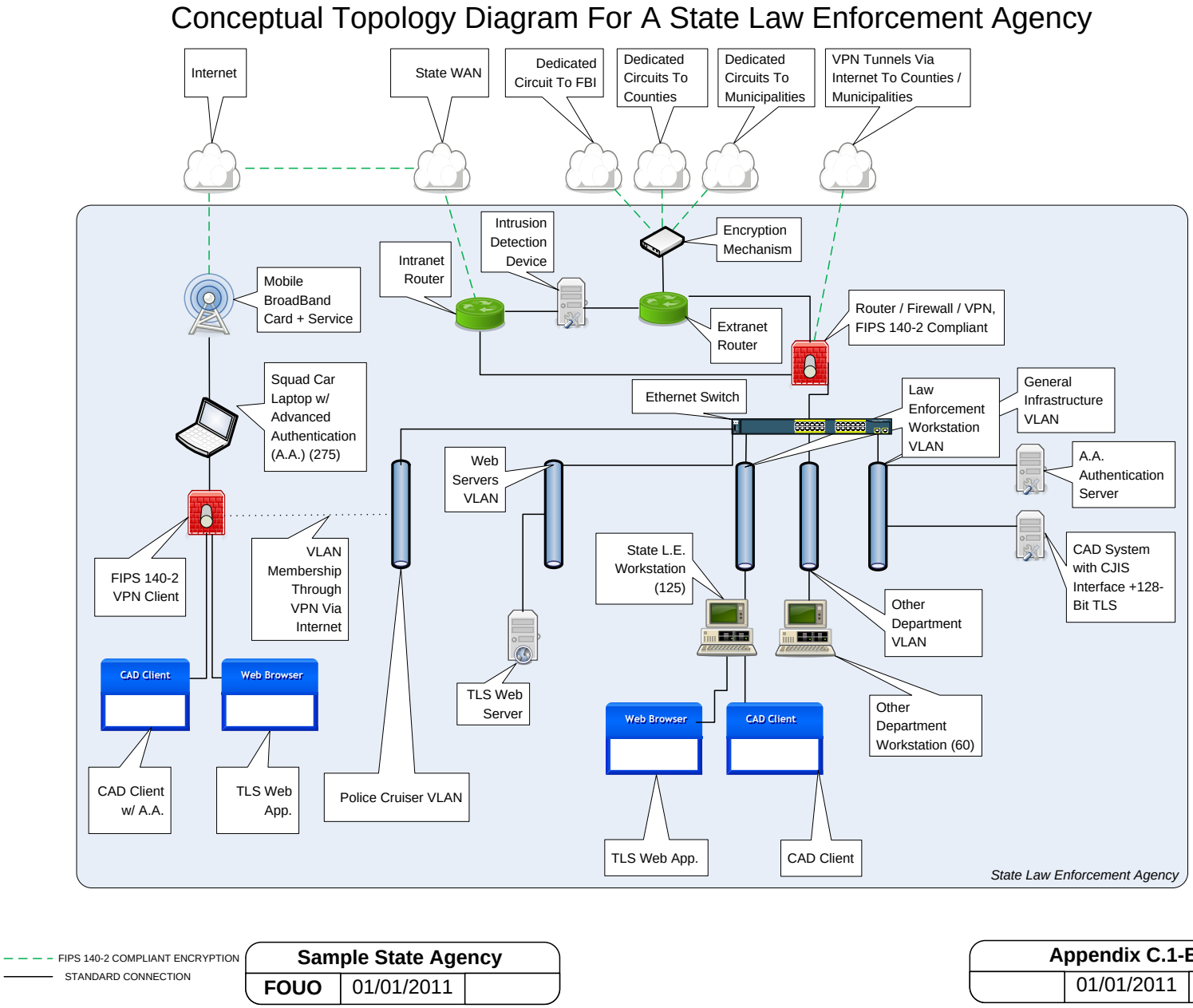
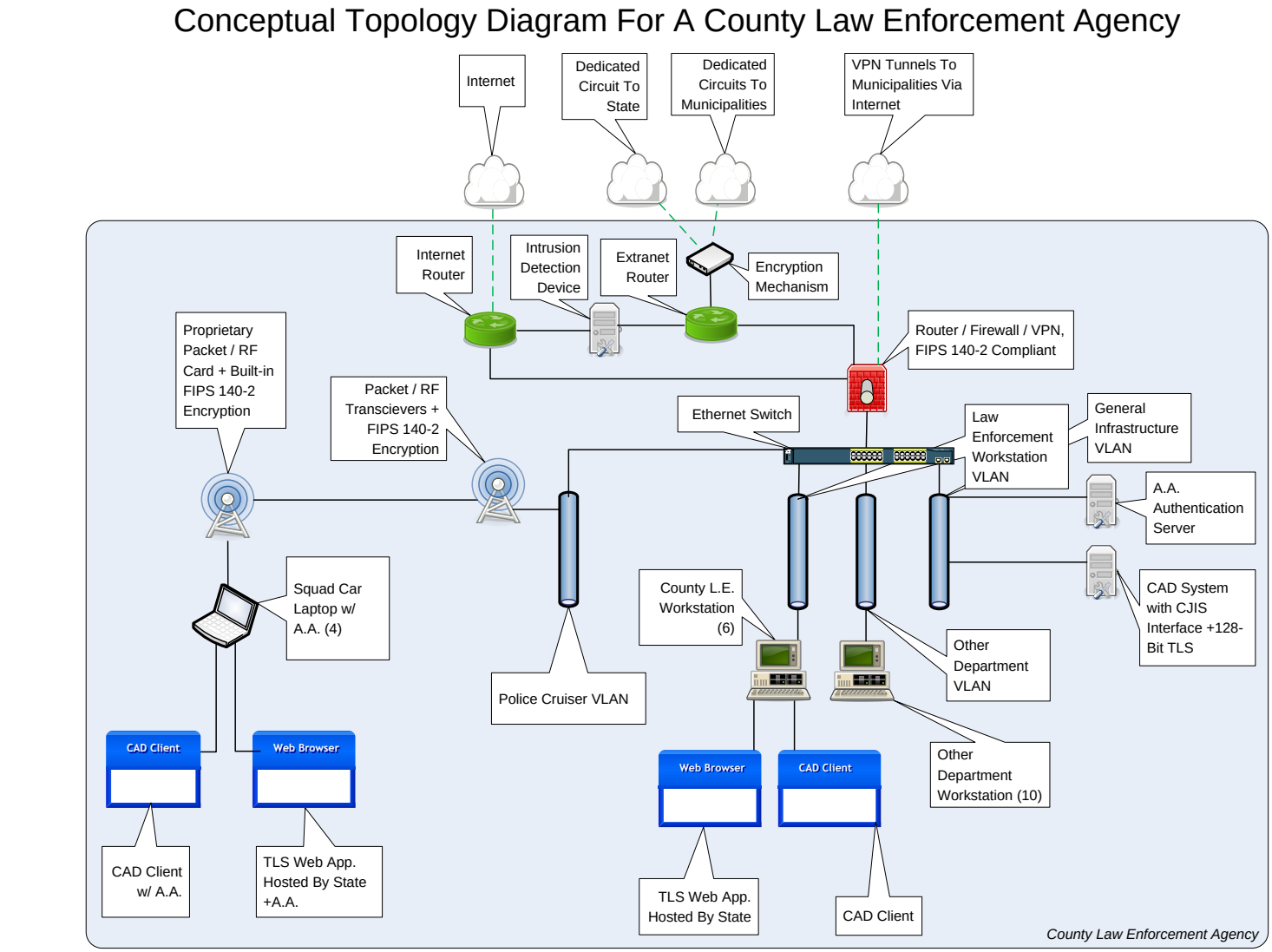


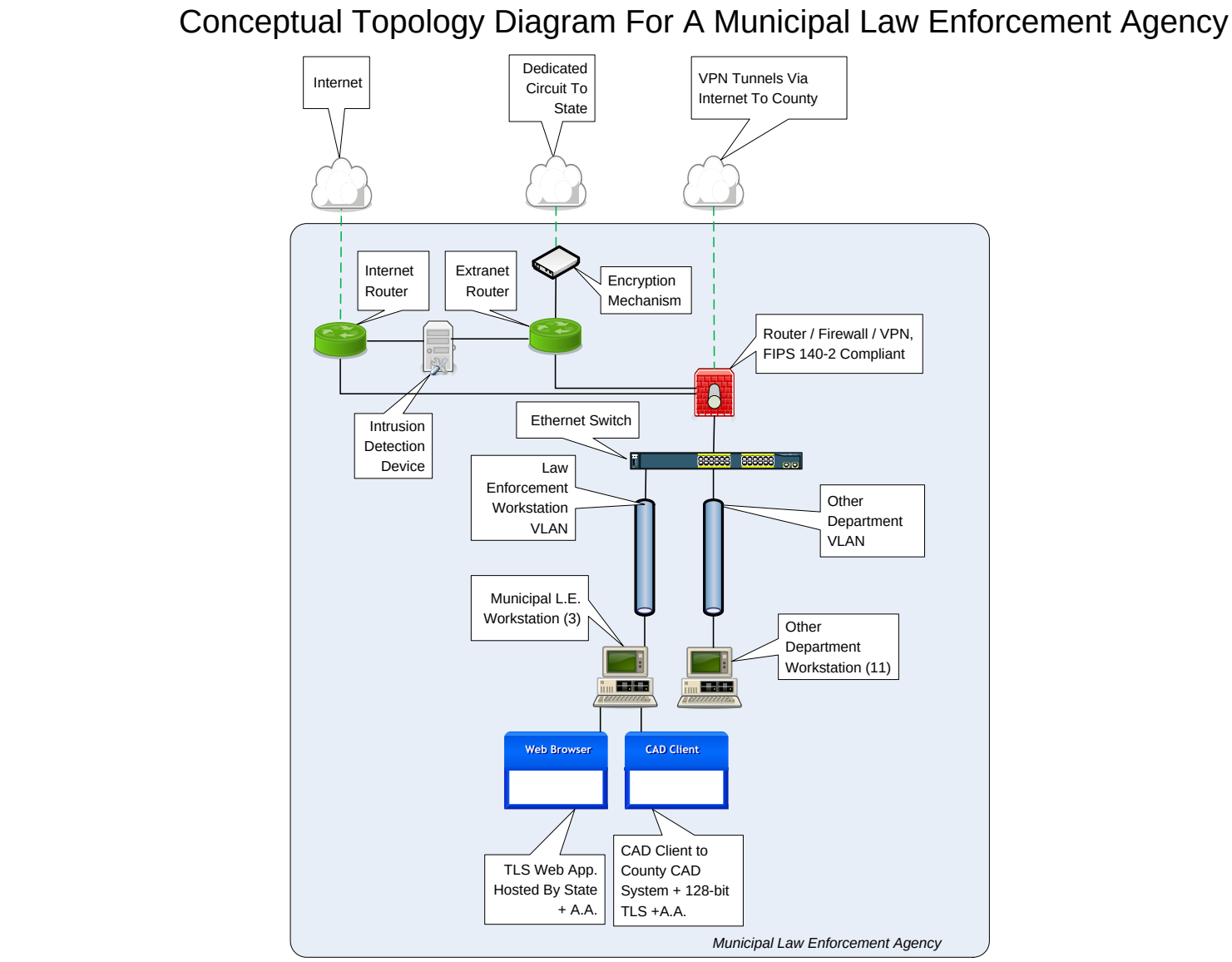
Figure C-1-C Conceptual Topology Diagram for a County Law Enforcement Agency



Sample County Agency		
FOUO	01/01/2011	

Appendix C.1-C		
	01/01/2011	

Figure C-1-D Conceptual Topology Diagram for a Municipal Law Enforcement Agency



APPENDIX D SAMPLE INFORMATION EXCHANGE AGREEMENTS

D.1 CJIS User Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)

SYSTEMS USER AGREEMENT

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities, as well as the noncriminal justice community, for licensing and employment purposes. These services are administered and maintained by the FBI CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) and its administrator for CJIS data, the CJIS Systems Officer (CSO). The CJIS Systems include, but are not limited to: the Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEx); Law Enforcement Enterprise Portal; and the National Instant Criminal Background Check System (NICS).

The FBI CJIS Division provides the following services to its users, as applicable:

1. Operational, technical, and investigative assistance.

2. Telecommunication lines to state, federal, and regulatory interfaces.

3. Legal and legislative review of matters pertaining to all CJIS Systems.

4. Timely information on all aspects of all CJIS Systems and other related programs by means of operating manuals, code manuals, technical and operational updates, various newsletters, information letters, frequently asked questions, and other relevant documents.

5. Training assistance and up-to-date materials provided to each CSO, NICS Point of Contact (POC), state Compact Officer, State Administrator, Information Security Officer (ISO), and other appropriate personnel.

6. Ongoing assistance to Systems' users through meetings and briefings with the CSO**s**, State Administrators, Compact Officers, ISOs, and NICS State POCs to discuss operational and policy issues.

7. Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS programs.

8. National Crime Prevention and Privacy Compact Administrative Office through which states and other authorized users may submit issues concerning the noncriminal justice use of the III System.

9. Annual NICS Users Conference.

10. Audit.

11. Staff research assistance.

PART 1

The purpose behind a designated CSO is to unify responsibility for Systems user discipline and to ensure adherence to established procedures and policies within each signatory state/territory/tribal agency and by each federal user. This agreement outlines the responsibilities of each CSO as they relate to all CJIS Systems and other related CJIS administered programs. These individuals are ultimately responsible for planning necessary hardware, software, funding, and training for access to all CJIS Systems.

To ensure continued access as set forth above, the CSA agrees to adhere to all applicable CJIS policies including, but not limited to, the following:

1. The signatory state/tribal agency will provide fingerprints that meet submission criteria for all qualifying arrests. In addition, states/tribal agencies will make their records available for interstate exchange for criminal justice and other authorized purposes unless restricted by state/tribal law, and, where applicable, continue to move toward participation in the III and, upon ratification of the National Crime Prevention and Privacy Compact, the National Fingerprint File.

2. Appropriate and reasonable quality assurance procedures; e.g., hit confirmation, audits for record timeliness, and validation, must be in place to ensure that only complete, accurate, and valid information is maintained in the CJIS Systems.

3. Biannual file synchronization of information entered into the III by participating states.

4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history

records. Additionally, each CSO must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

5. Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.

6. Training - Each agency shall be responsible for training requirements, including compliance with operator training mandates.

7. Integrity of the Systems - Each agency shall be responsible for maintaining the integrity of the system in accordance with FBI CJIS Division/state/federal/tribal policies to ensure only authorized terminal access; only authorized transaction submission; and proper handling and dissemination of CJI. Each agency shall also be responsible for computer security incident reporting as required by the *CJIS Security Policy*.

The following documents are incorporated by reference and made part of this agreement for CSA users:

1. Bylaws for the CJIS Advisory Policy Board and Working Groups.

2. CJIS Security Policy.

3. Interstate Identification Index Operational and Technical Manual, National Fingerprint File Operations Plan, NCIC 2000 Operating Manual, UCR Handbook-NIBRS Edition, and National Incident-Based Reporting System Volumes 1, 2, and 4.

4. National Crime Prevention and Privacy Compact, 42 United States Code (U.S.C.) §14616.

5. NCIC Standards and UCR Standards, as recommended by the CJIS Advisory Policy Board.

6. The National Fingerprint File Qualification Requirements.

7. Title 28, Code of Federal Regulations, Parts 20 and 25, §50.12, and Chapter IX.

8. Electronic Fingerprint Transmission Specifications.

9. Other relevant documents, to include: NCIC Technical and Operational Updates, CJIS Information Letters, NICS User Manual, NICS Interface Control Document.

10. Applicable federal, state, and tribal laws and regulations.

PART 2

Additionally, there are authorized federal regulatory recipients and other authorized users that provide electronic fingerprint submissions through a CJIS Wide Area Network (WAN) connection (or other approved form of electronic connection) to the CJIS Division that are required to comply with the following CJIS policies:

1. The authorized user will provide fingerprints that meet submission criteria and apply appropriate and reasonable quality assurance procedures.

2. Security - Each agency is responsible for appropriate security measures as applicable to physical security of communication equipment; personnel security to include background screening requirements; technical security to protect against unauthorized use; and security of criminal history records.

3. Audit - Each authorized user shall be responsible for complying with all audit requirements for CJIS Systems. Additionally, each authorized user is subject to a triennial audit by the CJIS Division Audit staff.

4. Training - Each authorized user receiving criminal history record information shall be responsible for training requirements, including compliance with proper handling of criminal history records.

The following documents are incorporated by reference and made part of this agreement for non-CSA authorized users:

1. CJIS Security Policy.

2. National Crime Prevention and Privacy Compact, 42 U.S.C. §14616.

3. Title 28, Code of Federal Regulations, Parts 20 and 25, § 50.12, and Chapter IX.

4. Other relevant documents, to include CJIS Information Letters.

5. Applicable federal, state, and tribal laws and regulations.

GENERAL PROVISIONS

Funding:

Unless otherwise agreed in writing, each party shall bear its own costs in relation to this agreement. Expenditures will be subject to federal and state budgetary processes and availability of funds pursuant to applicable laws and regulations. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

Termination:

1. All activities of the parties under this agreement will be carried out in accordance to the above-described provisions.

2. This agreement may be amended or terminated by the mutual written consent of the parties authorized representatives.

3. Either party may terminate this agreement upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

    a. The parties will continue participation, financial or otherwise, up to the effective date of termination.

    b. Each party will pay the costs it incurs as a result of termination.

    c. All information and rights therein received under the provisions of this agreement prior to the termination will be retained by the parties, subject to the provisions of this agreement.

ACKNOWLEDGMENT AND CERTIFICATION

As a CSO or CJIS WAN Official (or other CJIS authorized official), I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS Systems users to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in, or obtained by means of, the CJIS Systems. I further acknowledge that failure to comply with these duties and responsibilities may result in the imposition of sanctions against the offending state/agency; other federal, tribal, state, and local criminal justice users; and approved noncriminal justice users with System access, whether direct or indirect. The Director of the FBI (or the National Crime Prevention and Privacy Compact Council), may approve sanctions to include the termination of CJIS services.

I hereby certify that I am familiar with all applicable documents that are made part of this agreement and to all applicable federal and state laws and regulations relevant to the receipt and dissemination of documents provided through the CJIS Systems.

This agreement is a formal expression of the purpose and intent of both parties and is effective when signed. It may be amended by the deletion or modification of any provision contained therein, or by the addition of new provisions, after written concurrence of both parties. The "Acknowledgment and Certification" is being executed by the CSO or CJIS WAN Official (or other CJIS authorized official) in both an individual and representative capacity**.** Accordingly, this agreement will remain in effect after the CSO or CJIS WAN Official (or other CJIS authorized official) vacates his/her position or until it is affirmatively amended or rescinded in writing. This agreement does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

SYSTEMS USER AGREEMENT

Please execute either Part 1 or Part 2

PART 1

_____ Date: _____

CJIS Systems Officer

_____

Printed Name/Title

CONCURRENCE OF CSA HEAD:

_____ Date: _____

CSA Head

_____

Printed Name/Title

PART 2

_____ Date: _____

CJIS WAN Official (or other CJIS Authorized Official)

_____

Printed Name/Title

CONCURRENCE OF CJIS WAN AGENCY HEAD:

_____ Date: _____

CJIS WAN Agency Head

_____

Printed Name/Title

FBI CJIS DIVISION:

_____ Date: _____

[Name]

Assistant Director

FBI CJIS Division

* The FBI Designated Federal Officer should be notified when a CSO or other CJIS WAN/authorized Official vacates his/her position. The name and telephone number of the Acting CSO or other CJIS WAN/authorized Official, and when known, the name and telephone number of the new CSO or other CJIS WAN/authorized Official, should be provided. Revised: 05/03/2006

D.2 Management Control Agreement

Management Control Agreement

Pursuant to the CJIS Security Policy, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the state network (Network Name) for the interstate exchange of criminal history/criminal justice information, the (Criminal Justice Agency) shall have the authority, via managed control, to set, maintain, and enforce:

(1) Priorities.
(2) Standards for the selection, supervision, and termination of personnel access to Criminal Justice Information (CJI).
(3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
(4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
(5) Compliance with all rules and regulations of the (Criminal Justice Agency) Policies and CJIS Security Policy in the operation of all information received.

"…management control of the criminal justice function remains solely with the Criminal Justice Agency." Section 5.1.1.4

This agreement covers the overall supervision of all (Criminal Justice Agency) systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any (Criminal Justice Agency) system to include NCIC Programs that may be subsequently designed and/or implemented within the (Criminal Justice Agency).

_____ _____
John Smith, CIO Date
Any State Department of Administration

_____ _____
Joan Brown, CIO Date
(Criminal Justice Agency)

D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

(Insert Name of Requesting Organization)

FOR

THE ESTABLISHMENT AND ACCOMMODATION OF
THIRD-PARTY CONNECTIVITY TO THE
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION'S WIDE AREA NETWORK

1. PURPOSE: This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI) and **(insert requesting organization's name)**, hereinafter referred to as the "parties," memorializes each party's responsibilities with regard to establishing connectivity to records services accessible via the Wide Area Network (WAN) of the FBI's Criminal Justice Information Services (CJIS) Division.

2. BACKGROUND: The requesting organization, **(insert requesting organization's name)**, being approved for access to systems of records accessible via the CJIS WAN, desires connectivity to the CJIS WAN or via a secure Virtual Private Network (VPN) Connection (Internet) to the CJIS WAN. The CJIS Division has created a framework for accommodating such requests based on the type of connection.

In preparing for such non-CJIS-funded connectivity to the CJIS WAN, the parties plan to acquire, configure, and place needed communications equipment at suitable sites and to make electronic connections to the appropriate systems of records via the CJIS WAN.

To ensure that there is a clear understanding between the parties regarding their respective roles in this process, this MOU memorializes each party's responsibilities regarding the development, operation, and maintenance of third-party connectivity to the CJIS WAN. Unless otherwise contained in an associated contract, the enclosed terms apply. If there is a conflict between terms and provisions contained in both the contract and this MOU, the contract will prevail.

3. AUTHORITY: The FBI is entering into this MOU under the authority provided by Title 28, United States Code (U.S.C.), Section 534; 42 U.S.C. § 14616; and/or Title 28, Code of Federal Regulations, Part 906.

4. SCOPE:

a. The CJIS Division agrees to:

i. Provide the requesting organization with a "CJIS WAN Third-Party Connectivity Package" that will detail connectivity requirements and options compatible with the CJIS Division's WAN architecture upon receipt of a signed nondisclosure statement.

ii. Configure the requesting organization’s connection termination equipment suite at Clarksburg, West Virginia, and prepare it for deployment or shipment under the CJIS WAN option. In the Secure VPN arrangement only, the third party will develop, configure, manage, and maintain its network connectivity to its preferred service provider.

iii. Work with the requesting organization to install the connection termination equipment suite and verify connectivity.

iv. Perform installation and/or routine maintenance on the requesting organization’s third-party dedicated CJIS WAN connection termination equipment after coordinating with the requesting organization’s designated point of contact (POC) and during a time when the CJIS Division's technical personnel are near the requesting organization’s site.

v. Perform periodic monitoring and troubleshooting of the requesting organization’s CJIS WAN connection termination equipment. Software patches will be maintained on the dedicated CJIS WAN connected network equipment only. Under the Secure VPN option, no availability or data thru-put rates will be guaranteed.

vi. Provide 24 hours a day, 7 days a week uninterrupted monitoring from the CJIS Division's Network Operations Center.

vii. Provide information regarding potential hardware end-of-life replacement cycles to the requesting organization for its budgeting purposes.

viii. Maintain third-party dedicated CJIS WAN connection termination equipment as if in the CJIS Division's operational environment.

ix. Update the appropriate software on the requesting organization's dedicated connection termination equipment connected to the CJIS WAN (i.e., Cisco Internetwork Operating System, SafeNet frame relay encryptor firmware, etc.) pursuant to the requesting organization's authorized maintenance contracts.

x. Provide a POC and telephone number for MOU-related issues.

b. The **(insert requesting organization's name)** agrees to:

i. Coordinate requests for third-party connectivity to the CJIS WAN or the Secure VPN with the CJIS Division's POC.

ii. Purchase hardware and software that are compatible with the CJIS WAN.

iii. Pay for the telecommunications infrastructure that supports its connection to the CJIS WAN or Secure VPN.

iv. Maintain telecommunication infrastructure in support of Secure VPN connectivity.

v. Provide any/all hardware and software replacements and upgrades as mutually agreed to by the parties.

vi. Pay for all telecommunication requirements related to its connectivity.

vii. Provide required information for dedicated service relating to Data Link Connection Identifiers, Circuit Identifier, Permanent Virtual Circuit Identifiers, Local Exchange Carrier Identifier, POC, location, etc., as determined by the parties.

viii. Transport the CJIS WAN connection termination equipment suite to the CJIS Division for configuration and preparation for deployment under the dedicated service option.

ix. Provide registered Internet Protocol information to be used by the requesting organization's system to the CJIS Division.

x. Provide the CJIS Division with six months advance notice or stated amount of time for testing activities (i.e., disaster recovery exercises).

xi. Provide the CJIS Division with applicable equipment maintenance contract numbers and level of service verifications needed to perform software upgrades on connection termination equipment.

xii. Provide the CJIS Division with applicable software upgrade and patch images (or information allowing the CJIS Division to access such images).

xiii. Transport only official, authorized traffic over the Secure VPN.

xiv. Provide a POC and telephone number for MOU-related issues.

5. FUNDING: There are no reimbursable expenses associated with this level of support. Each party will fund its own activities unless otherwise agreed to in writing. This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of understanding between the parties hereto of the nature of the relationship for the connectivity efforts. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the above language in no way implies that Congress will appropriate funds for such expenditures.

6. SETTLEMENT OF DISPUTES: Disagreements between the parties arising under or relating to this MOU will be resolved only by consultation between the parties and will not be referred to any other person or entity for settlement.

7. SECURITY: It is the intent of the parties that the actions carried out under this MOU will be conducted at the unclassified level. No classified information will be provided or generated under this MOU.

8. AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION:

a. All activities of the parties under this MOU will be carried out in accordance with the above - described provisions.

b. This MOU may be amended or terminated by the mutual written consent of the parties' authorized representatives.

c. Either party may terminate this MOU upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

i. The parties will continue participation, financial or otherwise, up to the effective date of the termination.

ii. Each party will pay the costs it incurs as a result of the termination.

iii. All information and rights therein received under the provisions of this MOU prior to the termination will be retained by the parties, subject to the provisions of this MOU.

9. FORCE AND EFFECT: This MOU, which consists of nine numbered sections, will enter into effect upon signature of the parties and will remain in effect until terminated. The parties should review the contents of this MOU annually to determine whether there is a need for the deletion, addition, or amendment of any provision. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The foregoing represents the understandings reached between the parties.

FOR THE FEDERAL BUREAU OF INVESTIGATION

_____ _____

[Name] Date

Assistant Director

Criminal Justice Information Services Division

FOR THE (insert requesting organization name)

_____ _____

Date

D.4 Interagency Connection Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)

Wide Area Network (WAN) USER AGREEMENT

BY INTERIM REMOTE LATENT USERS

The responsibility of the FBI CJIS Division is to provide state-of-the-art identification and information services to the local, state, federal, and international criminal justice communities, as well as the civil community for licensing and employment purposes. The data provided by the information systems administered and maintained by the FBI CJIS Division are routed to and managed in cooperation with the designated interface agency official. This information includes, but is not limited to, the Interstate Identification Index (III), National Crime Information Center (NCIC), Uniform Crime Reporting (UCR)/National Incident-Based Reporting System (NIBRS), and the Integrated Automated Fingerprint Identification System (IAFIS) programs.

In order to fulfill this responsibility, the FBI CJIS Division provides the following services to its users:

- Operational, technical, and investigative assistance;
- Telecommunications lines to local, state, federal and authorized interfaces;
- Legal and legislative review of matters pertaining to IAFIS, CJIS WAN and other related services;
- Timely information on all aspects of IAFIS, CJIS WAN, and other related programs by means of technical and operational updates, various newsletters, and other relative documents;
- Shared management through the CJIS Advisory Process and the Compact Council;
- Training assistance and up-to-date materials provided to each designated agency official, and;
- Audit.

The concept behind a designated interface agency official is to unify responsibility for system user discipline and ensure adherence to system procedures and policies within each interface agency. These individuals are ultimately responsible for planning necessary hardware, software, funding, training, and the administration of policy and procedures including security and integrity for complete access to CJIS related systems and CJIS WAN related data services by authorized agencies.

The following documents and procedures are incorporated by reference and made part of this agreement:

- *CJIS Security Policy*;
- *Title 28, Code of Federal Regulations, Part 20*;
- Computer Incident Response Capability (CIRC);
- Applicable federal and state laws and regulations.

To ensure continued access as set forth above, the designated interface agency agrees to adhere to all CJIS policies, including, but not limited to, the following:

1. The signatory criminal agency will provide fingerprints for all qualifying arrests either via electronic submission or fingerprint card that meet submission criteria. In addition, the agency will make their records available for interstate exchange for criminal justice and other authorized purposes.

2. The signatory civil agency with legislative authority will provide all qualifying fingerprints via electronic submission or fingerprint card that meet submission criteria.

3. Appropriate and reasonable quality assurance procedures must be in place to ensure that only complete, accurate, and valid information is maintained in the system.

4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunications lines; Interim Distributed Imaging System (IDIS) equipment shall remain stand-alone

devices and be used only for authorized purposes; personnel security to meet background screening requirements; technical security to protect against unauthorized use; data security, dissemination, and logging for audit purposes; and actual security of criminal history records. Additionally, each agency must establish an information security structure that provides for an Information Security Officer (ISO) or a security point of contact.

5. Audit - Each agency shall be responsible for complying with the appropriate audit requirements.

6. Training - Each agency shall be responsible for training requirements, including compliance with training mandates.

7. Integrity of the system shall be in accordance with FBI CJIS Division and interface agency policies. Computer incident reporting shall be implemented.

Until states are able to provide remote latent connectivity to their respective latent communities via a state WAN connection, the CJIS Division may provide direct connectivity to IAFIS via a dial-up connection or through the Combined DNA Index System (CODIS) and/or National Integrated Ballistics Information Network (NIBIN) connections. When a state implements a latent management system and is able to provide intrastate connectivity and subsequent forwarding to IAFIS, this agreement may be terminated. Such termination notice will be provided in writing by either the FBI or the state CJIS Systems Agency.

It is the responsibility of the local remote latent user to develop or acquire an IAFIS compatible workstation. These workstations may use the software provided by the FBI or develop their own software, provided it is IAFIS compliant.

The CJIS Division will provide the approved modem and encryptors required for each dial-up connection to IAFIS. The CJIS Communication Technologies Unit will configure and test the encryptors before they are provided to the user. Users requesting remote latent connectivity through an existing CODIS and/or NIBIN connection must receive verification from the FBI that there are a sufficient number of Ethernet ports on the router to accommodate the request.

If at any time search limits are imposed by the CJIS Division, these individual agency connections will be counted toward the total state allotment.

ACKNOWLEDGMENT AND CERTIFICATION

As a CJIS WAN interface agency official serving in the CJIS system, I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS system users in order to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in or obtained by means of the CJIS system. I further acknowledge that a failure to comply with these duties and responsibilities may subject our agency to various sanctions adopted by the CJIS Advisory Policy Board and approved by the Director of the FBI. These sanctions may include the termination of CJIS service.

As the designated CJIS WAN interface agency official serving in the CJIS system, I hereby certify that I am familiar with the contents of the *Title 28, Code of Federal Regulations, Part 20; CJIS Security Policy; Computer Incident Response Capability;* and applicable federal or state laws and regulations applied to IAFIS and CJIS WAN Programs for the dissemination of criminal history records for criminal and noncriminal justice purposes.

*_____ _____

Signature Print or Type

CJIS WAN Agency Official Date

CONCURRENCE OF FEDERAL/REGULATORY AGENCY HEAD OR STATE CJIS SYSTEMS OFFICER (CSO):

*_____ _____

Signature Print or Type

*_____ _____

Title Date

State CSO

FBI CJIS DIVISION:

_____

Signature – [Name]

Assistant Director _____

Title Date

* If there is a change in the CJIS WAN interface agency official, the FBI Designated Federal Employee must be notified in writing 30 days prior to the change.

5/27/2004 UA modification reflects change in CTO title to CSO.

APPENDIX E SECURITY FORUMS AND ORGANIZATIONAL ENTITIES

Online Security Forums / Organizational Entities
AntiOnline
Black Hat
CIO.com
CSO Online
CyberSpeak Podcast
FBI Criminal Justice Information Services Division (CJIS)
Forrester Security Forum
Forum of Incident Response and Security Teams (FIRST)
Information Security Forum (ISF)
Information Systems Audit and Control Association (ISACA)
Information Systems Security Association (ISSA)
Infosyssec
International Organization for Standardization (ISO)
International Information Systems Security Certification Consortium, Inc. $(ISC)^2$
Metasploit
Microsoft Developer Network (MSDN) Information Security
National Institute of Standards and Technology (NIST)
Open Web Application Security Project (OWASP)
SANS (SysAdmin, Audit, Network, Security) Institute
SC Magazine
Schneier.com
Security Focus
The Register
US Computer Emergency Response Team (CERT)
US DoJ Computer Crime and Intellectual Property Section (CCIPS)

APPENDIX F SAMPLE FORMS

This appendix contains sample forms.

F.1 Security Incident Response Form

FBI CJIS DIVISION

INFORMATION SECURITY OFFICER (ISO)

SECURITY INCIDENT REPORTING FORM

NAME OF PERSON REPORTING THE INCIDENT: _____

DATE OF REPORT: _____ (mm/dd/yyyy)

DATE OF INCIDENT: _____ (mm/dd/yyyy)

POINT(S) OF CONTACT (Include Phone/Extension/Email): _____

_____

LOCATION(S) OF INCIDENT: _____

INCIDENT DESCRIPTION: _____

_____

SYSTEM(S) AFFECTED: _____

_____

SYSTEM(S) AFFECTED (e.g. CAD, RMS, file server, etc.): _____

_____

METHOD OF DETECTION: _____

ACTIONS TAKEN/RESOLUTION: _____

_____

_____

Copies To:

John C. Weatherly
(FBI CJIS Division ISO)
1000 Custer Hollow Road
Clarksburg, WV 26306-0102
(304) 625-3660
iso@fbi.gov

APPENDIX G BEST PRACTICES

G.1 Virtualization

Virtualization

This appendix documents security considerations for implementing and operating virtual environments that process, store, and/or transmit Criminal Justice Information.

The FBI CJIS ISO has fielded several inquiries from various states requesting guidance on implementing virtual environments within their data centers. With the proliferation of virtual environments across industry in general there is a realistic expectation that FBI CJIS Auditors will encounter virtual environments during the upcoming year. Criminal Justice Agencies (CJAs) and Noncriminal Justice Agencies (NCJAs) alike need to understand and appreciate the foundation of security protection measures required for virtual environments.

From Microsoft's Introduction to Windows Server 2008
http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx:

> *"Server virtualization, also known as hardware virtualization, is a hot topic in the IT world because of the potential for serious economic benefits. Server virtualization enables multiple operating systems to run on a single physical machine as virtual machines (VMs). With server virtualization, you can consolidate workloads across multiple underutilized server machines onto a smaller number of machines. Fewer physical machines can lead to reduced costs through lower hardware, energy, and management overhead, plus the creation of a more dynamic IT infrastructure."*

From a trade publication, kernelthread.com
http://www.kernelthread.com/publications/virtualization/:

> *"Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others."*

From an Open Source Software developer
http://www.kallasoft.com/pc-hardware-virtualization-basics/:

> *"Virtualization refers to virtualizing hardware in software, allowing multiple operating systems, or images, to run concurrently on the same hardware. There are two main types of virtualization software:*
>
> - *"Type-1 Hypervisor, which runs 'bare-metal' (on top of the hardware)*
> - *"Type-2 Hypervisor which requires a separate application to run within an operating system*

"Type1 hypervisors usually offer the best in efficiency, while Type-2 hypervisors allow for greater support of hardware that can be provided by the operating system. For the developer, power user, and small business IT professionals, virtualization offers the same basic idea of collapsing multiple physical boxes into one. For instance, a small business can run a web server and an Exchange server without the need for two boxes. Developers and power users can use the ability to contain different development environments without the need to modify their main operating system. Big businesses can also benefit from virtualization by allowing software maintenance to be run and tested on a separate image on hardware without having to take down the main production system."

Industry leaders and niche developers are bringing more products to market every day. The following article excerpts, all posted during September 2008, on www.virtualization.com are examples of industry offerings.

"Microsoft and Novell partnered together for joint virtualization solution. Microsoft and Novell are announcing the availability of a joint virtualization solution optimized for customers running mixed-source environments. The joint offering includes SUSE Linux Enterprise Server configured and tested as an optimized guest operating system running on Windows Sever 2008 Hyper-V, and is fully support by both companies' channel partners. The offering provides customers with the first complete, fully supported and optimized virtualization solution to span Windows and Linux environments."

"Sun Microsystems today account the availability of Sun xVM Server software and Sun xVM Ops Center 2.0, key components in its strategy. Sun also announced the addition of comprehensive services and support for Sun xVM Server software and xVM Ops Center 2.0 to its virtualization suite of services. Additionally, Sun launched xVMserver.org, a new open source community, where developers can download the first source code bundle for SunxVM Server software and contribute to the direction and development of the product."

"NetEx, specialist in high-speed data transport over TCP, today announced Vistual HyperIP bandwidth optimization solutions for VMware environments that deliver a threefold to tenfold increase in data replication performance. Virtual HyperIP is a software-based Data Transport Optimizer that operates on the VMware ESX server and boosts the performance of storage replication applications from vendors such as EMC, NetApp, Symantec, IBM, Data Domain, and FalconStor. Virtual HyperIP mitigates TCP performance issues that are common when moving data over wide –area network (WAN) connections because of bandwidth restrictions, latency due to distance and/or router hop counts, packet loss and network errors. Like the company's award-winning appliance-based HyperIP, Virtual HyperIP eliminates these issues with an innovative software design developed specifically to accelerate traffic over an IP based network."

From several sources, particularly:

http://www.windowsecurity.com/articles/security-virutalization.html
http://csrc.nist.gov/publications/drafts/6--=64rev2/draft-sp800-64-Revision2.pdf

Virtualization provides several benefits:

- Make better use of under-utilized servers by consolidating to fewer machines saving on hardware, environmental costs, management, and administration of the server infrastructure.
- Legacy applications unable to run on newer hardware and/or operating systems can be loaded into a virtual environment – replicating the legacy environment.
- Provides for isolated portions of a server where trusted and untrusted applications can be ran simultaneously – enabling hot standbys for failover.
- Enables existing operating systems to run on shared memory multiprocessors.
- System migration, backup, and recovery are easier and more manageable.

Virtualization also introduces several vulnerabilities:

- Host Dependent.
- If the host machine has a problem then all the VMs could potentially terminate.
- Compromise of the host makes it possible to take down the client servers hosted on the primary host machine.
- If the virtual network is compromised then the client is also compromised.
- Client share and host share can be exploited on both instances. Potentially this can lead to files being copied to the share that fill up the drive.

These vulnerabilities can be mitigated by the following factors:

- Apply "least privilege" technique to reduce the attack surface area of the virtual environment and access to the physical environment.
- Configuration and patch management of the virtual machine and host, i.e. Keep operating systems and application patches up to date on both virtual machines and hosts.
- Install the minimum applications needed on host machines.
- Practice isolation from host and virtual machine.
- Install and keep updated antivirus on virtual machines and the host.
- Segregation of administrative duties for host and versions.
- Audit logging as well as exporting and storing the logs outside the virtual environment.
- Encrypting network traffic between the virtual machine and host IDS and IPS monitoring.
- Firewall each virtual machine from each other and ensure that only allowed protocols will transact.

G.2 Voice over Internet Protocol

Voice over Internet Protocol (VoIP)

Attribution:

The following information has been extracted from NIST Special Publication 800-58, Security Considerations for Voice over IP Systems.

Definitions:

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) - A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Summary:

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are alluring since the typical cost to operate VoIP is less than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol services. Unfortunately, installing a VoIP network is not a simple "plug-and-play" procedure. There are myriad security concerns, cost issues with new networking hardware requirements, and overarching quality of service (QoS) factors that have to be considered carefully.

What are some of the advantages of VoIP?

a. Cost – a VoIP system is usually cheaper to operate than an equivalent office telephone system with a Private Branch Exchange and conventional telephone service.

b. Integration with other services – innovative services are emerging that allow customers to combine web access with telephone features through a single PC or terminal. For example, a sales representative could discuss products with a customer using the company's web site. In addition, the VoIP system may be integrated with video across the Internet, providing a teleconferencing facility.

What are some of the disadvantages of VoIP?

a. Startup cost – although VoIP can be expected to save money in the long run, the initial installation can be complex and expensive. In addition, a single standard has not yet emerged for many aspects of VoIP, so an organization must plan to support more than one standard, or expect to make relatively frequent changes as the VoIP field develops.

b. Security – the flexibility of VoIP comes at a price: added complexity in securing voice and data. Because VoIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VoIP system than a conventional voice telephone system or PBX.

VoIP Risks, Threats, and Vulnerabilities

This section details some of the potential threats and vulnerabilities in a VoIP environment, including vulnerabilities of both VoIP phones and switches. Threat discussion is included because the varieties of threats faced by an organization determine the priorities in securing its communications equipment. Not all threats are present in all organizations. A commercial firm may be concerned primarily with toll fraud, while a government agency may need to prevent disclosure of sensitive information because of privacy or national security concerns. Information security risks can be broadly categorized into the following three types: confidentiality, integrity, and availability, (which can be remembered with the mnemonic "CIA"). Additional risks relevant to switches are fraud and risk of physical damage to the switch, physical network, or telephone extensions.

Packet networks depend for their successful operation on a large number of configurable parameters: IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VoIP specific software such as Call Managers and other programs used to place and route calls. Many of these network parameters are established dynamically every time a network component is restarted, or when a VoIP telephone is restarted or added to the network. Because there are so many places in a network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack.

Vulnerabilities described in this section are generic and may not apply to all systems, but investigations by NIST and other organizations have found these vulnerabilities in a number of VoIP systems. In addition, this list is not exhaustive; systems may have security weaknesses that are not included in the list. For each potential vulnerability, a recommendation is included to eliminate or reduce the risk of compromise.

Confidentiality and Privacy

Confidentiality refers to the need to keep information secure and private. For home computer users, this category includes confidential memoranda, financial information, and security information such as passwords. In a telecommunications switch, eavesdropping on conversations is an obvious concern, but the confidentiality of other information on the switch must be protected to defend against toll fraud, voice and data interception, and denial of service attacks. Network IP addresses, operating system type, telephone extension to IP address mappings, and communication protocols are all examples of information that, while not critical as individual pieces of data, can make an attacker's job easier.

With conventional telephones, eavesdropping usually requires either physical access to tap a line, or penetration of a switch. Attempting physical access increases the intruder's risk of being discovered, and conventional PBXs have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers increase dramatically, because of the many nodes in a packet network.

Switch Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. This vulnerability also allows for wiretapping conversations on the network with port mirroring or bridging. An attacker with access to the switch administrative interface can mirror all packets on one port to another, allowing the indirect and unnoticeable interception of all communications. Failing to change default passwords is one of the most common errors made by inexperienced users.

REMEDIATION: If possible, remote access to the graphical user interface should be disabled to prevent the interception of plaintext administration sessions. Some devices provide the option of a direct USB connection in addition to remote access through a web browser interface. Disabling port mirroring on the switch should also be considered.

Classical Wiretap Vulnerability

Attaching a packet capture tool or protocol analyzer to the VoIP network segment makes it easy to intercept voice traffic.

REMEDIATION: A good physical security policy for the deployment environment is a general first step to maintaining confidentiality. Disabling the hubs on IP Phones as well as developing an alarm system for notifying the administrator when an IP Phone has been disconnected will allow for the possible detection of this kind of attack.

ARP Cache Poisoning and ARP Floods

Because many systems have little authentication, an intruder may be able to log onto a computer on the VoIP network segment, and then send ARP commands corrupting ARP caches on sender(s) of desired traffic, then activate IP. An ARP flood attack on the switch could render the network vulnerable to conversation eavesdropping. Broadcasting ARP replies blind is sufficient to corrupt many ARP caches. Corrupting the ARP cache makes it possible to re-route traffic to intercept voice and data traffic.

REMEDIATION: Use authentication mechanisms wherever possible and limit physical access to the VoIP network segment.

Web Server interfaces

Both VoIP switches and voice terminals are likely to have a web server interface for remote or local administration. An attacker may be able to sniff plaintext HTTP packets to gain confidential information. This would require access to the local network on which the server resides.

REMEDIATION: If possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

IP Phone Netmask Vulnerability

A similar effect of the ARP Cache Vulnerability can be achieved by assigning a subnet mask and router address to the phone crafted to cause most or all of the packets it transmits to be sent to an attacker's MAC address. Again, standard IP forwarding makes the intrusion all but undetectable.

REMEDIATION: A firewall filtering mechanism can reduce the probability of this attack. Remote access to IP phones is a severe risk.

Extension to IP Address Mapping Vulnerability

Discovering the IP address corresponding to any extension requires only calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered. Knowing the IP address of a particular extension is not a compromise in itself, but makes it easier to accomplish other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it will be easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's job may be much more difficult to accomplish and require much longer, possibly resulting in the attack being discovered.

REMEDIATION: Disabling the hub on the IP Phone will prevent this kind of attack. However, it is a rather simple task to turn the hub back on.

Integrity Issues

Integrity of information means that information remains unaltered by unauthorized users. For example, most users want to ensure that bank account numbers cannot be changed by anyone else, or that passwords are changed only by the user or an authorized security administrator. Telecommunication switches must protect the integrity of their system data and configuration. Because of the richness of feature sets available on switches, an attacker who can compromise the system configuration can accomplish nearly any other goal. For example, an ordinary extension could be re-assigned into a pool of phones that supervisors can listen in on or record conversations for quality control purposes. Damaging or deleting information about the IP network used by a VoIP switch results in an immediate denial of service.

The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for intruders to use on their next visit. For this reason, the security system must be carefully protected. Integrity threats include any in which system functions or data may be corrupted, either accidentally or as a result of malicious actions. Misuse may involve legitimate users (i.e. insiders performing unauthorized operations) or intruders.

A legitimate user may perform an incorrect, or unauthorized, operations function (e.g., by mistake or out of malice) and may cause deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.

Intrusion - An intruder may masquerade as a legitimate user and access an operations port of the switch. There are a number of serious intrusion threats. For example, the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:

- Disclosing confidential data
- Causing service deterioration by modifying the switch software
- Crashing the switch
- Removing all traces of the intrusion (e.g., modifying the security log) so that it may not be readily detected

Insecure state - At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:

- After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, even though new passwords are not yet assigned.) The same may happen at the time of a disaster recovery.
- At the time of installation the switch may be vulnerable until the default security features have been replaced.

DHCP Server Insertion Attack

It is often possible to change the configuration of a target phone by exploiting the DHCP response race when the IP phone boots. As soon as the IP phone requests a DHCP response, a rogue DHCP server can initiate a response with data fields containing false information.

This attack allows for possible man in the middle attacks on the IP-media gateway, and IP Phones. Many methods exist with the potential to reboot the phone remotely, e.g. “social engineering”, ping flood, MAC spoofing (probably SNMP hooks, etc.).

REMEDIATION: If possible, use static IP addresses for the IP Phones. This will remove the necessity of using a DHCP server. Further, using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing this traffic only from the legitimate server.

TFTP Server Insertion Attack

It is possible to change the configuration of a target phone by exploiting the TFTP response race when the IP phone is resetting. A rogue TFTP server can supply spurious

information before the legitimate server is able to respond to a request. This attack allows an attacker to change the configuration of an IP Phone.

REMEDIATION: Using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing such traffic only from the legitimate server. Organizations looking to deploy VoIP systems should look for IP Phone instruments that can download signed binary files.

Availability and Denial of Service

Availability refers to the notion that information and services be available for use when needed. Availability is the most obvious risk for a switch. Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration or even denial of service or functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service. A voice over IP system may have additional vulnerabilities with Internet connections. Because intrusion detection systems fail to intercept a significant percentage of Internet based attacks, attackers may be able to bring down VoIP systems by exploiting weaknesses in Internet protocols and services.

Any network may be vulnerable to denial of service attacks, simply by overloading the capacity of the system. With VoIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

CPU Resource Consumption Attack without any account information.

An attacker with remote terminal access to the server may be able to force a system restart (shutdown all/restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP Phones may reboot as a result of this attack.

In addition to producing a system outage, the restart may not restore uncommitted changes or, in some cases, may restore default passwords, which would introduce intrusion vulnerabilities.

REMEDIATION: The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof his MAC and IP address, circumventing the firewall protection.

Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. Similarly, VoIP telephones often have default keypad sequences that can be used to unlock and modify network information.

This vulnerability would allow an attacker to control the topology of the network remotely, allowing for not only complete denial of service to the network, but also a port mirroring attack to the attacker's location, giving the ability to intercept any other conversations taking place over the same switch. Further, the switch may have a web server interface, providing an attacker with the ability to disrupt the network without advance knowledge of switch operations and commands. In most systems, telephones download their configuration data on startup using TFTP or similar protocols. The configuration specifies the IP addresses for Call Manager nodes, so an attacker could substitute another IP address pointing to a call manager that would allow eavesdropping or traffic analysis.

REMEDIATION: Changing the default password is crucial. Moreover, the graphical user interface should be disabled to prevent the interception of plaintext administration sessions.

Exploitable software flaws

Like other types of software, VoIP systems have been found to have vulnerabilities due to buffer overflows and improper packet header handling. These flaws typically occur because the software is not validating critical information properly. For example, a short integer may be used as a table index without checking whether the parameter passed to the function exceeds 32,767, resulting in invalid memory accesses or crashing of the system.

Exploitable software flaws typically result in two types of vulnerabilities: denial of service or revelation of critical system parameters. Denial of service can often be implemented remotely, by passing packets with specially constructed headers that cause the software to fail. In some cases the system can be crashed, producing a memory dump in which an intruder can find IP addresses of critical system nodes, passwords, or other security-relevant information. In addition, buffer overflows that allow the introduction of malicious code have been found in VoIP software, as in other applications.

REMEDIATION: These problems require action from the software vendor, and distribution of patches to administrators. Intruders monitor announcements of vulnerabilities, knowing that many organizations require days or weeks to update their software. Regular checking for software updates and patches is essential to reducing these vulnerabilities. Automated patch handling can assist in reducing the window of opportunity for intruders to exploit known software vulnerabilities.

Account Lockout Vulnerability

An attacker will be able to provide several incorrect login attempts at the telnet prompt until the account becomes locked out. (This problem is common to most password-protected systems, because it prevents attackers from repeating login attempts until the correct password is found by trying all possible combinations.)

The account is unable to connect to the machine for the set lockout time.

REMEDIATION: If remote access is not available, this problem can be solved with physical access control.

NIST Recommendations.

Because of the integration of voice and data in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. In particular, start with these general guidelines, recognizing that practical considerations, such as cost or legal requirements, may require adjustments for the organization:

1. Develop appropriate network architecture.

- Separate voice and data on logically different networks if feasible. Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate DHCP servers for each, to ease the incorporation of intrusion detection and VoIP firewall protection at the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component. Strong authentication of clients towards a gateway often presents difficulties, particularly in key management. Here, access control mechanisms and policy enforcement may help.

- A mechanism to allow VoIP traffic through firewalls is required. There are a variety of protocol dependent and independent solutions, including application level gateways (ALGs) for VoIP protocols, Session Border Controllers, or other standards-based solutions when they mature.

- Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. (This may not be practical when multimedia protocol inherent security or lower layer security is applied, e.g., H.235 Annex D for integrity provision or TLS to protect SIP signaling).

- Use IPsec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.

- If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPsec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network has been encrypted. Newer IP phones are able to provide Advanced Encryption System (AES) encryption at reasonable cost. Note that Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer

and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

2. Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.

VoIP can provide more flexible service at lower cost, but there are significant tradeoffs that must be considered. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied in to the data network, resulting in additional security weaknesses and avenues of attack (see VoIP Risks, Threats, and Vulnerabilities section for more detailed discussion of vulnerabilities of VoIP and their relation to data network vulnerabilities).

Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative instability of VoIP technology compared with established telephony systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. The public switched telephone network is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed, and maintained, will be at greater risk if based on VoIP.

3. Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.

Unlike traditional telephone connections, which are tied to a physical location, VoIP's packet switched technology allows a particular number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the tradeoff is that this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the 911 dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Agencies must carefully evaluate E-911 issues in planning for VoIP deployment.

4. Agencies should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.

Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect with a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis (i.e., determine which parties are communicating). Agencies therefore should ensure that adequate physical security is in place to restrict access to VoIP network components. Physical security measures, including barriers, locks, access control systems, and guards, are the first line of defense. Agencies must make sure that the proper physical countermeasures are in place to mitigate some of

the biggest risks such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking this means that installation of a sniffer could result in not just data but all voice communications being intercepted.

5. VoIP-ready firewalls and other appropriate protection mechanisms should be employed. Agencies must enable, use, and routinely test the security features that are included in VoIP systems.

Because of the inherent vulnerabilities (e.g. susceptibility to packet sniffing) when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

6. If practical, "softphone" systems, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern.

Worms, viruses, and other malicious software are extraordinarily common on PCs connected to the internet, and very difficult to defend against. Well-known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user's knowledge, even if the user does nothing more than visit a compromised web site. Malicious software attached to email messages can also be installed without the user's knowledge, in some cases even if the user does not open the attachment. These vulnerabilities result in unacceptably high risks in the use of "softphones", for most applications. In addition, because PCs are necessarily on the data network, using a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

7. If mobile units are to be integrated with the VoIP system, use products implementing WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent WiFi Protected Access (WPA), a snapshot of the ongoing 802.11i standard, offers significant improvements in security, and can aid the integration of wireless technology with VoIP. NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, the 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access, or other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for Federal agencies that have determined that certain information must be protected via cryptographic means. As currently defined, neither WEP nor WPA meets the FIPS 140-2 standard. In these cases, it will be necessary to employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport Level Security (TLS) or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect information, regardless of whether the nonvalidated data link security protocols are used.

8. Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

Although legal issues regarding VoIP are beyond the scope of this document, readers should be aware that laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may be different from those for conventional telephone systems. Agencies should review these issues with their legal advisors. See Section 2.5 for more on these issues.

G.3 Cloud Computing

Cloud Computing

Purpose:

This paper is provided to define and describe cloud computing, discuss CJIS Security Policy (CSP) compliance, detail security and privacy, and provide general recommendations.

Attribution:

- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing (Dec. 2011)
- NIST SP 800-145, the NIST Definition of Cloud Computing (Sept. 2011)
- NIST SP 800-146, Cloud Computing Synopsis and Recommendations (May 2011)
- CJIS Security Policy, Version 5.0

Definitions and Terms:

Cloud computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), software, and information.

Cloud subscriber – A person or organization that is a customer of a cloud

Cloud client – A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a subscriber

Cloud provider – An organization that provides cloud services

Summary:

With many law enforcement agencies looking for ways to attain greater efficiency while grappling with reduced budgets, the idea of cloud computing to maintain data and applications is a viable business solution. But the unique security and legal characteristics of law enforcement agencies means any migration to cloud services may be challenging. Anytime the security of information and transactions must be maintained, as it must be with access to the FBI's CJIS systems and the protection of Criminal Justice Information (CJI), security and policy compliance concerns are bound to arise.

Cloud computing has become a popular and sometimes contentious topic of discussion for both the private and public sectors. This is in part because of the difficulty in describing cloud computing in general terms, because it is not a single kind of system. The "cloud" spans a spectrum of underlying technologies, configuration possibilities, service and deployment models. Cloud computing offers the ability to conveniently rent access to fully featured applications, software development and deployment environments, and computing infrastructure assets - such as network-accessible data storage and processing from a cloud service provider.

One of the benefits of cloud computing is the ability to outsource many of the technical functions agencies may not want to perform for various reasons. Ultimately, the move to cloud computing is a business and security risk decision in which the following relevant factors are given proper consideration:

- readiness of existing applications for cloud deployment
- transition costs
- life-cycle costs
- maturity of service orientation in existing infrastructure
- security and privacy requirements – federal, state, and local

Achieving CJIS Security Policy Compliance:

The question that is often asked is, "Can an Agency be compliant with the CJIS Security Policy and also cloud compute?"

Because the CJIS Security Policy is device and architecture independent (per CSP Section 2.2), the answer is yes, and this can be accomplished— assuming the vendor of the cloud technology is able to meet the existing requirements of the CJIS Security Policy.

There are security challenges that must be addressed if CJI is to be sent into or through, stored within, or accessed from the cloud.

Admittedly, the existing CJIS Security Policy requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic disbursement of their personnel; however, the requirements aren't new to vendors serving the criminal justice community and many vendors have been successfully meeting the Policy requirements for years. Even so, they are the minimum security requirements which will provide an acceptable level of assurance that law enforcement and personally identifiable information (PII) will be protected when shared with other law enforcement agencies across the nation.

General CJIS Security Policy Applicability Questions

Before tackling these challenges, the cloud subscriber should first be aware of what security and legal requirements they are subject to prior to entering into any agreement with a cloud provider. Asking the following general questions will help frame the process of determining compliance with the existing requirements of the CJIS Security Policy.

- Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (5.5.6 Remote Access)

- Will advanced authentication (AA) be required for access to CJI within a cloud environment? (5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale)

- Does/do any cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (5.9.1 Physically Secure Location)

- Are the encryption requirements being met? (5.10.1.2 Encryption)
    - Who will be providing the encryption as required in the CJIS Security Policy (client or cloud service provider)? *Note: individuals with access to the keys can decrypt the stored files and therefore have access to unencrypted CJI.*
    - Is the data encrypted while at rest and in transit?

- What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response)
    - Will the cloud subscriber be notified of any incident?
    - If CJI is compromised, what are the notification and response procedures?

- Is the cloud service provider a private contractor/vendor?
    - If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI? (5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Contractors and Vendors)

- Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? *Note: Cloud facilities such as datacenters in which CJI will be stored or processed should be audited as would any other datacenter housing and processing CJI.* (5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA)

- How will event and content logging be handled? (5.4 Policy Area 4, Auditing and Accountability)
    - Will the cloud service provider handle the events and content logging required by the CJIS Security Policy and provide that upon request?
    - What are the cloud service provider's responsibilities with regard to media protection and destruction? (5.8 Policy Area 8: Media Protection)

Ultimately, the goal is to remain committed to using technology in its information sharing processes, but not at the sacrifice of the security of the information with which it has been entrusted. As stated in the CJIS Security Policy, device and architecture independence permits the use of cloud computing, but the security requirements do not change.

Cloud Utilization Scenarios

1. Encrypted CJI in a Cloud Environment–Key Management Control, Security Awareness Training, and Personnel Controls

   Prior to permitting CJI to be stored or traverse through a cloud environment, the agency should ensure proper encryption key management control procedures are implemented to determine who has access and control over the encryption keys. Proper key management control is vital to CJI security as those individuals (agency or cloud employees) with access to the keys can decrypt the stored files, and therefore, have unescorted access to unencrypted CJI. This means all those individuals must be subjected to security awareness training (CJIS Security Policy section 5.2) and must meet personnel security (CJIS Security Policy Section 5.12) requirements as individuals with unescorted access to unencrypted CJI.

   Note: As a best security practice, the CJIS ISO Program does not recommend allowing the cloud service provider access to the encryption keys used to protect CJI. However, it may not always be reasonable to expect the agency, criminal justice or noncriminal justice, to accomplish this task.

   a. Scenario 1–Agency Stores CJI in a Cloud:
      A CJA stores encrypted CJI (Backup files and drives) in a cloud service provider's environment. To access CJI, the agency will extract the CJI from the cloud to its local machine, and then decrypt the CJI. The CJI is processed, re-encrypted, and then re-uploaded to the cloud environment for storage. In this scenario, the agency always encrypts the CJI prior to placing it in the cloud and only authorized users of the agency have access to the encryption keys. Since the agency maintains the encryption keys, the cloud service provider employees would not need to undergo fingerprint-based background checks, nor have security awareness training. These requirements are negated, because only authorized personnel with access to the keys have the ability to view this CJI in an unencrypted form.

   b. Scenario 2–Agency Accesses CJI While in a Cloud:

A CJA stores CJI (files and drives) in a cloud service provider's environment, but as part of daily operations authorized users will remotely access the encrypted CJI in the cloud. The user will decrypt the CJI while it is in the cloud's virtual environment, process the data, and then re-encrypt the data prior to ending the remote session. The agency maintains the keys and the cloud service provider does not have access to the encryption keys. However, since the CJI is decrypted within the cloud's virtual environment, any administrative personnel employed by the cloud provider having the ability to access the virtual environment must be identified and subjected to security awareness training and personnel security controls as described in the CJIS Security Policy.

c. Scenario 3–CJI Impact from a Cloud Datacenter Critical Systems Crash–Core Dump[2] Recovery:
A CJA utilizes a cloud service provider (IaaS or PaaS) to store CJI and remotely accesses the environment to process CJI. During normal operation, the cloud provider experiences systems outages within the datacenter in which CJI is processed and stored. The cloud provider's administrators need to repair the systems and restore service using data from a core dump to return to normal operations. The cloud service provider as part of the Service Level Agreement (SLA) with the CJA has been authorized to maintain the encryption keys in order respond to such an event. The cloud administrators with such access have underwent fingerprint-based background checks and security awareness training. This allows the cloud administrators to decrypt CJI so that it is written to the core dump files for restoration following the system outage. CJI, however, is encrypted at all times except when part of the core dump files. As part of the SLA, the cloud service provider has agreed to treat the core dump files as CJI to ensure all protection are in place in compliance with the CJIS Security Policy.

Note: Writing encrypted data to a core dump corrupts the data and makes it unusable because the key no longer decrypts the data. This is problematic when attempting to recover encrypted data written to a core dump. The CJA could have ensured the cloud provider exclude encrypted data (CJI) from the core dump, but chose against it.

The Cloud Model Explained:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

[2] Core Dump - A file of a computer's documented memory of when a program or computer crashed. The file consists of the recorded status of the working memory at an explicit time, usually close to when the system crashed or when the program ended atypically as it presents the risk that the system failure would ensure the loss of the encrypted data.

The cloud model as defined by NIST consists of five essential characteristics, offers the option of three service models, and may be deployed via any of four deployment models as shown in Figure 1 below:

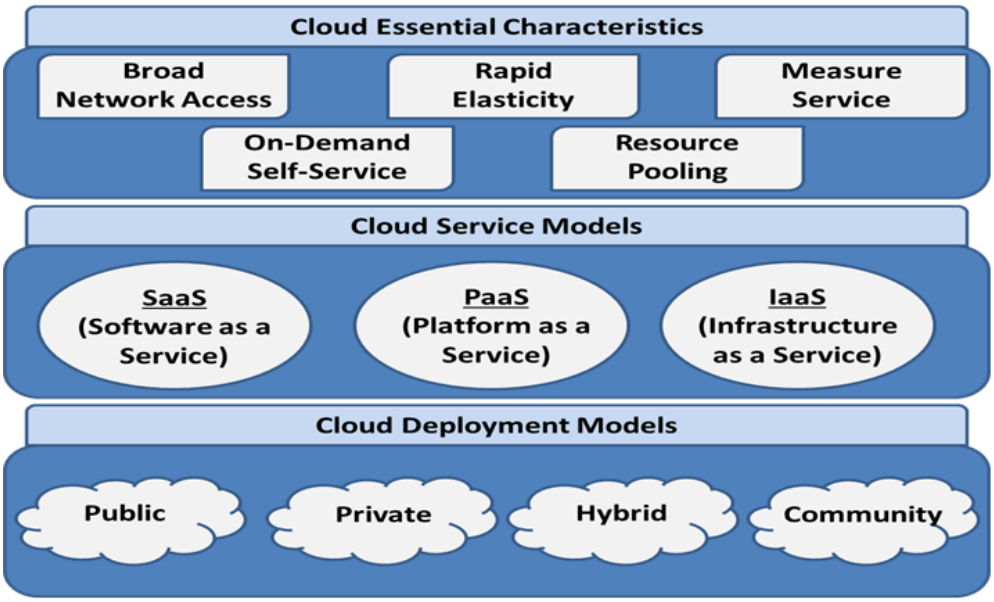


Figure 1 - Visual Depiction of the NIST Cloud Computing Definition

Essential Characteristics:

On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in which the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction

(e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability* at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

** Typically this is done on a pay-per-use or charge-per-use basis.*

Deployment Models:

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Service Models:

Software as a Service (SaaS)

This model provides the consumer the capability to use the provider's applications running on a cloud infrastructure*.

> ** A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.*

The SaaS service model is often referred to as "Software deployed as a hosted service and accessed over the Internet."

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

When using the SaaS service model it should be understood that the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS)

This model provides the consumer the capability to deploy consumer-created or acquired applications* created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure.

> ** This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.*

When using the PaaS service model the consumer may have control over the deployed applications and possibly configuration settings for the application-hosting environment, but does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.

Infrastructure as a Service (IaaS)

This model provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications.

When using the IaaS service model the consumer may have control over operating systems, storage, and deployed applications; and possibly limited control of select

networking components (e.g., host firewalls), but does not manage or control the underlying cloud infrastructure.

Key Security and Privacy Issues:

Although the emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing and experimenting with available cloud provider platforms and associated technologies. The sections below highlight privacy and security-related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service models.

Because cloud computing has grown out of an amalgamation of technologies, including service oriented architecture, virtualization, Web 2.0, and utility computing, many of the privacy and security issues involved can be viewed as known problems cast in a new setting. The importance of their combined effect in this setting, however, should not be discounted. Public cloud computing does represent a thought-provoking paradigm shift from conventional norms to an open organizational infrastructure—*at the extreme, displacing applications from one organization's infrastructure to the infrastructure of another organization, where the applications of potential adversaries may also operate.*

Governance

Governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.

Dealing with cloud services requires attention to the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met. Ensuring systems are secure and risk is managed is challenging in any environment and even more daunting with cloud computing. Audit mechanisms and tools should be in place to determine how data is stored, protected, and used, to validate services, and to verify policy enforcement. A risk management program should also be in place that is flexible enough to deal with the continuously evolving and shifting risk landscape.

Compliance

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing.

Law and Regulations

Cloud providers are becoming more sensitive to legal and regulatory concerns, and may be willing to commit to store and process data in specific jurisdictions and apply required safeguards for security and privacy. However, the degree to which they will accept liability in their service agreements, for exposure of content under their control, remains to be seen. Even so, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.

Data Location

One of the most common compliance issues facing an organization is data location. A characteristic of many cloud computing services is that data is stored redundantly in multiple physical locations and detailed information about the location of an organization's data is unavailable or not disclosed to the service consumer. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. External audits and security certifications can alleviate this issue to some extent, but they are not a panacea.

When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations.

Electronic Discovery

The capabilities and processes of a cloud provider, such as the form in which data is maintained and the electronic discovery-related tools available, affect the ability of the organization to meet its obligations in a cost effective, timely, and compliant manner. A cloud provider's archival capabilities may not preserve the original metadata as expected, causing spoliation (i.e., the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation), which could negatively impact litigation.

Trust

Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and privacy, and in doing so, confers a high level of trust onto the cloud provider. At the same time, federal agencies have a responsibility to protect information and information systems commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction, regardless of whether the information is collected or maintained by or on behalf of the agency; or whether the information systems are used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

Insider Access

Data processed or stored outside the physical confines of an organization, its firewall, and other security controls bring with it an inherent level of risk. The insider security threat is a well-known issue for most organizations. Incidents may involve various types of fraud, sabotage of information resources, and theft of sensitive information.

Data Ownership

The organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust and privacy of data. The continuing controversy over privacy and data ownership rights for social networking users illustrates the impact that ambiguous terms can have on the parties involved.

Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; that the cloud provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the organization's data for its own purposes; and that the cloud provider does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the cloud provider.

Visibility

Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Transition to public cloud services entails a transfer of responsibility to the cloud provider for securing portions of the system on which the organization's data and applications operate.

Ancillary Data

While the focus of attention in cloud computing is mainly on protecting application data, cloud providers also hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks.

Risk Management

Assessing and managing risk in systems that use cloud services can be a challenge. With cloud-based services, some subsystems or subsystem components fall outside of the direct control of a client organization. Many organizations are more comfortable with risk when they have greater control over the processes and equipment involved. Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls. Ultimately, if the level of trust in the service falls below expectations and the organization is unable to employ compensating controls, it must either reject the service or accept a greater degree of risk.

Architecture

The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers for any specific service model. It is important to understand the technologies the cloud provider uses to provision services and the implications the technical controls involved have on security and privacy of the system throughout its lifecycle. With such information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to assess and manage risk.

Identity and Access Management

Data sensitivity and privacy of information have become increasingly an area of concern for organizations. The identity proofing and authentication aspects of identity management entail the use, maintenance, and protection of PII collected from users. Preventing unauthorized access to information resources in the cloud is also a major consideration. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public cloud and extending or changing the existing framework to support cloud services may prove difficult.

Software Isolation

High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost

benefits and efficiencies due to economies of scale. Regardless of the service model and multi-tenant software architecture used, the computations of different consumers must be able to be carried out in isolation from one another, mainly through the use of logical separation mechanisms.

Data Protection

Data stored in a public cloud typically resides in a shared environment collocated with data from other customers. Organizations placing sensitive and regulated data into a public cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. Similar concerns exist for data migrated within or between clouds.

Value Concentration

Having data collocated with that of an organization with a high threat profile could also lead to a denial of service, as an unintended casualty from an attack targeted against that organization. Similarly, side effects from a physical attack against a high profile organization's cloud-based resources are also a possibility. For example, over the years, facilities of the Internal Revenue Service have attracted their share of attention from would-be attackers.

Data Isolation

Database environments used in cloud computing can vary significantly. Accordingly, various types of multi-tenant arrangements exist for databases. Each arrangement pools resources differently, offering different degrees of isolation and resource efficiency. Regardless of implementation decision, data must be secured while at rest, in transit, and in use, and access to the data must be controlled.

Data Sanitization

The data sanitization practices that a cloud provider implements have obvious implications for security. Sanitization involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of the media itself, to prevent unauthorized disclosure of information. Data sanitization also applies to backup copies made for recovery and restoration of service and residual data remaining upon termination of service.

In a public cloud computing environment, data from one consumer is physically collocated (e.g., in an IaaS data store) or commingled (e.g., in a SaaS database) with the data of other consumers, which can complicate matters. Service agreements should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle.

Encryption

Client end-to-end encryption (e.g. encryption/decryption occurs on the law enforcement controlled client prior to data entering the cloud and decryption occurs only on the client device after encrypted data is removed from the cloud service) with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data.

- May cause significant cloud service functionality limitations on available service types made available for sensitive data. This may also increase expenses to cover key items, such as key management and client software. Additionally, a number of specific SLA or contract clauses may be necessary for the implementation of client end-to end encryption.

Use of cloud services without end-to-end encryption implemented by the client is another option that would require cloud service provider participation in the encryption of data.

- This would require at least some cloud provider personnel to undergo personnel background screening and training.

- Specialized Service Level Agreements (SLA) and/or contractual clauses would be necessary to identify those personnel that may have access to unencrypted, sensitive data.

- Conducting the analysis and gaining approval of particular cloud service implementations not utilizing end-to-end encryption for sensitive law enforcement data may be costly and time consuming due to the high degree of technical complexity.

<u>Availability</u>

In simple terms, availability is the extent to which an organization's full set of computational resources is accessible and usable. Denial of service attacks, equipment outages, and natural disasters are all threats to availability. The concern is that most downtime is unplanned and can impact the mission of the organization. Some examples of unplanned service interruptions that cause concerns are:

- Temporary Outages
- Prolonged and Permanent Outages
- Denial of Service

Incident Response

The complexity of a cloud service can obscure recognition and analysis of incidents. Revising an organization's incident response plan to address differences between the organizational computing environment and a cloud computing environment is an important, but easy-to-overlook prerequisite to transitioning applications and data.

Data Availability

The availability of relevant data from event monitoring is essential for timely detection of security incidents. Cloud consumers are often confronted with extremely limited capabilities for detection of incidents in public cloud environments. The situation varies among cloud service models and cloud providers. For example, PaaS providers typically do not make event logs available to consumers, who are then left mainly with event data from self-deployed applications (e.g., via application logging). Similarly, SaaS consumers are completely dependent upon the cloud provider to provide event data such as activity logging, while IaaS consumers control more of the information stack and have access to associated event sources.

Incident Analysis and Resolution

An analysis to confirm the occurrence of an incident or determine the method of exploit needs to be performed quickly and with sufficient detail of documentation and care to ensure that traceability and integrity is maintained for subsequent use, if needed (e.g., a forensic copy of incident data for legal proceedings). Issues faced by cloud consumers when performing incident analysis include lack of detailed information about the architecture of the cloud relevant to an incident, lack of information about relevant event and data sources held by the cloud provider, ill-defined or vague incident handling responsibilities stipulated for the cloud provider, and limited capabilities for gathering and preserving pertinent data sources as evidence. Understanding and negotiating the provisions and procedures for incident response should be done before entering into a service contract, rather than as an afterthought.

General Recommendations:

A number of significant security and privacy issues were covered in the previous subsections. Table 1 summarizes those issues and related recommendations for organizations to follow when planning, reviewing, negotiating, or initiating a public cloud service outsourcing arrangement.

Table 1: Security and Privacy Issue Areas and Recommendations

Areas	Recommendations
Governance	• Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. • Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.
Compliance	• Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements. • Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. • Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.
Trust	• Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. • Establish clear, exclusive ownership rights over data. • Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system. • Continuously monitor the security state of the information system to support on-going risk management decisions.
Architecture	• Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.
Identity and Access Management	• Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.
Software Isolation	• Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.
Data Protection	• Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data.

	• Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value. • Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.
Availability	• Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements. • Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.
Incident Response	• Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization. • Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. • Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

G.4 Mobile Appendix

Mobile Appendix

Introduction

Mobile devices present a unique security challenge with regard to the correct application of CJIS Security Policy requirements. This appendix is intended to provide best practices based on industry standards and on methods to achieve policy compliance in mobile device employment scenarios. The technical methods used to achieve compliance with CJIS Security Policy will typically be different within the mobile environment than those used in fixed locations. Many of the security features and capabilities inherited by endpoint devices from the fixed environment are either not present or present in a different form in the mobile environment. Additionally, the basic technologies used in some types of mobile devices may adequately fulfill some of the CJIS Security Policy requirements which would require additional software or added features in a traditional fixed computing environment. Due to the complexity and rapid evolvement of the mobile environment, this Appendix will remain as device and vendor agnostic as practical, however certain key requirements for specific mobile operating systems will be identified for the major mobile operating systems (e.g. Apple iOS, Android) as the underlying technologies are fundamentally different and offer different levels of built-in compliance to CJIS Security Policy.

Sections within this appendix will provide recommendations regarding priorities and level of effort versus value of applying certain security controls in the mobile environment. These recommendations do not supersede or modify the requirements listed in the CJIS Security Policy, and are intended to describe the effect of inherent security functions and inherent device limitations in many mobile platforms that impact the application of policy elements in the mobile environment.

Mobile Device Risk Scenarios

There are multiple risk scenarios that may apply to mobile devices depending on the category of device (e.g. Laptop, Tablet, and 'Pocket sized' devices such as smartphones) and the methods of device connectivity (e.g. cellular service, WiFi + Cellular, WiFi only). Device category and method of connection define the technology types within the device which inherently affects the total level of compliance with CJIS Security Policy that can be obtained by the mobile device.

It is advisable for acquiring agencies to review the mobile device guidance in this Appendix prior to completing selection and acquisition of particular devices. Both the device category and connectivity methods installed and configured on the device will impact the overall risk scenario associated with the device and may significantly affect the effective cost to bring use of the device in compliance with the CJIS Security Policy. For instance, inclusion of cellular radios with the ability to remotely control a device significantly changes the risk scenario by allowing remote tracking, file deletion, and device management which could provide a higher level of CJIS Security Policy compliance than a WiFi only device that does not guarantee the ability to remotely manage the device. However, inclusion of cellular technology may significantly increase the initial device costs and incur ongoing subscription costs. Appropriate choices based on the intended use of the device along with the types and methods of Criminal Justice Information (CJI) data to be accessed could greatly reduce agency cost and enhance security.

Device Categories

This appendix defines risk levels for three categories of devices. Prior to reading individual sections of this Appendix, the agency should identify which device categories will apply to their employment scenario. If multiple categories of devices are employed, individual technical configurations and local policy will likely need to be defined for each category of device based on the risk inherent in the technical characteristics associated with each device category.

Laptop devices

The laptop device category includes mobile devices in a larger format that are transported either in a vehicle mount or a carrying case and include a monitor with attached keyboard. This includes all traditional laptop computers that utilize a 'traditional', full-featured operating system (e.g. Windows or a Linux variant). Also included in this category are 'tablet' type full-featured computers running a traditional full-featured operating system but without an attached keyboard. The main defining factor is the use of a full-featured operating system and a form factor too large to be carried in a pocket. In general, devices of this type connect via WiFi only, but may include an internal cellular access card in some cases.

The risks associated with this device type are similar to a standard desktop computer at the technical level, but are increased due to the potential to connect directly to the internet without the benefit of organizational network security layers (e.g. network firewall, IDS/IPS, network monitoring devices). There is also an increased risk of intentional device theft from vehicles or unsecure locations as these devices are too large to be carried on the authorized user's body. There may be increased risk from the limited technical ability to wipe or track a lost/stolen device depending on the particular technical means used for remote device connectivity (e.g. cellular or WiFi).

In general, the technical configurations for compliance with most of the CJIS Security Policy that is accomplished via the operating system (e.g. auditing, access control, etc) will remain consistent with normal fixed location computing systems for laptop devices, but some functions may operate in an unexpected manner due to lack of constant connectivity. Thorough testing of applied security policy elements within the expected mobile environments will help ensure the applied policy configurations remain effective and appropriate when applied to mobile laptop devices.

NOTE: Some newer devices running multi-function operating systems (e.g. Windows 8 or similar multi-mode operating systems) may exhibit technical features associated with both laptop and tablet device categories based on their current operating mode which may be reconfigured by the user on demand. If this is the case, it will be necessary to assess and configure multiple operating modes to be compliant with CJIS Security Policy on the device, or restrict the operating mode to one category of operation.

Tablet devices

The tablet device category includes larger format devices transported via vehicle mount or portfolio sized carry case that typically consist of a touch screen without attached keyboard. These devices utilize a limited-feature operating system (e.g. Apple iOS, Google Android, Windows mobile) that is inherently more resistant than a traditional operating system to certain types of network based technical attacks due to the limited-feature sets. Additionally, limited functionality operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers. This inherently limits the types of services that can

function effectively on the devices (e.g. traditional real-time anti-virus software) as the base operating system may not be designed to allow installed applications enhanced execution priority in the background and or the ability to examine the contents or communications associated within another application. However, this same design methodology significantly limits the vectors available for malware transmission and the device or application data actually accessible to malware if a device becomes infected.

Tablet devices will have different risks associated depending on the installed and configured methods for network access (e.g. 'always on cellular' vs. WiFi only). Physical risks associated with this category are similar to the laptop category for enhanced likelihood of intentional theft or device hijacking while unattended, while the technical risks are similar to the pocket device category.

Pocket devices/Handheld devices

The pocket/handheld device category is technically similar or identical to the tablet category and is primarily differentiated by device form factor. Pocket/handheld devices are characterized as having a limited functionality operating system and a small form factor intended for carry in a pocket or 'holster' attached to the body. The bulk of this category will be cellular 'smartphones' with integrated cellular data connectivity, however devices intended to be worn or carried on the body (e.g. portable fingerprint devices) may also be included in this category if they operate using a limited functionality operating system. Custom or specialty devices may meet the form factor distinction for this category, but operate using a full-feature operating system. In rare cases of this nature the employing agency should apply security guidance and principles in this appendix for both the laptop and pocket device categories.

Risks associated with this category are a reduced threat of theft to a stored devices (e.g. device left unattended in a vehicle) since these devices are typically carried continuously by the authorized user, but include a greater risk of temporary or permanent loss of control due to the device being misplaced by the authorized user.

Due to the installation of a limited functionality operating system, the technical threat to these devices via a network based attack is significantly lower than the laptop category, however, the threat of unauthorized access at the device level may be higher if the device is lost due to technical limits on multi-factor authentication to the operating system itself and practical limits to device passwords due to screen/software keyboard limitations.

NOTE: Data accessible on pocket or tablet devices simply through the entry of a single device PIN or password should not be considered secure due to the likelihood of enhanced password guessing based on fingerprints/smudges on the device touch screen. Any data stored on devices of these types should be protected within a separate secure container using Advanced Authentication.

Device Connectivity

There are three main categories of device connectivity that are associated with varying risk levels and threats to the devices. The Three categories are: Cellular Network Only (always on), WiFi Only (includes 'on demand' cellular), and Cellular (always on) + WiFi network. The risks associated with connectivity categories are general risks and may apply differently to any particular device at different points in its usage or lifecycle. Particular device configurations either through the operating system or a third-party mobile device management (MDM) system may be

able to significantly control and define which particular connectivity risks may be associated with a particular device.

Cellular Network Only (always on)

Cellular network connectivity is characterized by ‘always on’ network connection through the device internal radio to a cellular network provider. There is a reasonable assurance that devices with ‘always on’ cellular can be tracked, managed, or wiped remotely if lost or stolen. This will significantly reduce risks associated with loss of the device and attempted illicit access to the device. One important consideration for this risk category is characterization of the device as ‘always on’ or ‘on demand’. In effect the difference is typically a configuration setting, which in some cases may be changeable by the user. In particular most cellular smart phones contain ‘airplane’ mode settings that disable all internal radios allowing a user authenticated to the device operating system via password or personal identification number (PIN) to disable the cellular system. Access to this functionality may be disabled through the use of some MDM systems which would necessitate a complete power down of the device while carried on aircraft. Additionally, someone illicitly obtaining a device with properly configured password requirements and screen lock timeouts would be unlikely to guess the device password before the device was reported stolen in order for them to disable the cellular connection and prevent tracking or a remote wipe of the device.

Cellular networks do not allow for the same level of exposure of individual devices to random access from the internet. This significantly reduces the potential network based attack vectors that might reach a cellular connected device. The risk scenario in most cases from a network based attack would be similar to a device protected behind rudimentary network defenses (e.g. standard firewall but NOT advanced intrusion detection/prevention) Cellular device communications cannot typically be accessed by other ‘eavesdropping’ devices physically close to them without significant specialized equipment and can be considered well protected against network attacks below the nation/state level of technical capability by the hosting technical infrastructure and technology inherent in the device. However, network based attacks that utilize connections initiated by the user device may still succeed over the cellular infrastructure. For this reason, the technical protections inherent in the cellular infrastructure provide limited protection against user/device initiated actions (e.g. web surfing on a cellular connected web browser). Therefore, the protections provided by always on cellular connections are primarily in the ability to remotely access the mobile device for tracking or data deletion in case of device loss or compromise, which combined with a limited functionality device operating system, the protections are generally equivalent to a ‘personal firewall’ if properly configured and supported by a well-designed organizational infrastructure. However, that equivalency does not apply to full-featured operating systems connected through cellular infrastructure.

NOTE: It should be noted that a technically capable, intentional, thief knowingly obtaining an ‘always on’ cellular device for the purpose of data theft can physically disable the radio by utilizing a Faraday cage or similar external electromagnetic shield device while attempting to guess the device password. While technically possible these methods require specialized equipment and high technical expertise and would be very unlikely to be employed except for specifically targeted attacks. When always on cellular connectivity is combined with a robust incident reporting process and user training for rapid response to device loss or theft, the associated risks can be minimized.

WiFi only (includes ‘on-demand’ cellular)

WiFi only devices do not include cellular radios or include cellular radio that must be manually activated or 'connected' to the cellular network. They connect to the network or internet through WiFi 'hotspots' or external access points or manually to cellular networks. Some MDM or device configurations may be able to limit the types and specific WiFi access points the device can connect to, which may change the risk scenario of the device to a similar risk scenario as the Cellular Network Only scenario. However, if mobile devices are permitted (through technical and or policy decisions) to connect to any WiFi access point designated by the device user, the overall device risk scenario is high and the device may be accessible to a large number of potential network based attack vectors. Unrestricted WiFi access is not recommended on any agency owned device, but must be assumed to exist on any personally owned device authorized to access CJI. Significant compensating controls may be needed to ensure devices accessing CJI over 'public' WiFi access points are not susceptible to communications network eavesdropping, credential hijacking or any of the various potential man-in-the-middle attacks possible through access point spoofing. The communications security risks can be significantly mitigated by mandatory device configurations (e.g. MDM based policy) that only allow devices to connect to cryptographically verified agency controlled WiFi access points.

WiFi only or devices with 'on-demand' cellular access (e.g. user or event driven cellular access initiated from the device and not from a centralized management location) are significantly more at risk from data loss subsequent to device loss or theft as there is no guarantee the tracking or remote wipe can be initiated once the device is out of agency control. This can be mitigated by utilizing tracking/anti-theft products that require a periodic network connection to authorize access and perform automated device locking ('bricking') or remote wipe if network connections are not made within a specified period. Software of this nature is generally available for full-featured laptops but may not be available for limited-feature mobile operating systems.

Cellular (always on) + WiFi Network

This is a hybrid scenario that has become typical with most 'smartphones'. These devices contain both the always on cellular connection, but may also be configured to access local WiFi networks for enhanced bandwidth. In considering devices with these technical characteristics, the theft/loss risks are similar to the cellular only scenario (due to tracking and remote access through the cellular connection), while the data and network based risks must be considered to be similar to the WiFi scenario unless the capability of the device to connect to WiFi networks is limited by technology or policy to agency owned WiFi Access Points configured in accordance with the CJIS Security Policy. Careful consideration must be made to the particular configurations, management systems, and human oriented operational policies based on the particular technical capabilities and configurations of these types of devices.

Incident Handling (CJIS Security Policy Section 5.3)

Additional or enhanced incident reporting and handing procedures will need to be developed to cover mobile device operating scenarios. Various exploits and methods to compromise mobile devices require either specialized equipment or lengthy operations to implement. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface. However, parallel or special incident handling procedures with associated equipment or systems may need to be put in place to properly respond to incidents involving mobile devices. This section lists three areas where enhanced incident handling and

response processes may need to be implemented to ensure mobile device compliance to the incident handling policy in Section 5.3.

If personally owned devices are utilized within the environment in a Bring Your Own device (BYOD) scenario, specialized and costly incident handling procedures and processes may need to be developed to support compliance for those devices. The costs associated with enhanced incident handling procedures may need to be incorporated in the cost and risk based analysis to allow personally owned devices in the BYOD scenario, as the technical methods and risk to achieve compliance under BYOD scenarios may exceed any cost savings potentially achieved through BYOD.

Loss of device Control

Mobile device users should be trained and provided with explicit user actions in case positive control of a mobile device is lost for any period of time. Loss of positive control means the device is in the physical control of non-CJIS authorized individual or the device is left unattended in an unsecure location (e.g. counter of the coffee shop). Even if the device is recovered quickly there is significant risk that either the device settings could be tampered with or data on the device could be illicitly accessed. The level of detail and particular scenarios identified in the agency incident response plan should be consistent with the presence of persistent CJI on the device or the technical means used to access CJI from the device (e.g. ask the question: "Is it reasonable to assume CJI could be accessed") as well as the degree of device configuration control exercised by the user from the device main login. At a minimum, special incident handling procedures should be developed for the following scenarios:

- Device known to be locked, control loss of minimal duration
- Device lock state unknown at time of control loss, duration of loss minimal
- Device lock state unknown at time of control loss, duration of loss extended
- Device known to be unlocked at time of control loss, duration of loss more than momentary.

NOTE: Organizations should define appropriate time value criteria based on the operational environment for the above scenarios. For instance, a 'momentary' loss of control might be considered a matter of seconds in a situation where no one could reasonably have accessed the device, while 'minimal' durations might include a few minutes of time and 'extended' periods would be any time longer than a few minutes.

Other scenarios should be addressed as appropriate to the intended device employment, with explicit user and organizational actions identified based on the device technologies and any organizational management capabilities.

Total Loss of device

Incident response scenarios for the total loss of the device should be developed based on the methods/storage of CJI on the device, the lock state of the device at time of loss (known locked, known unlocked, or unknown), and the technical methods available for remote tracking or wiping of the device. It is critical to implement incident handling procedures quickly in this case. Remote wipe functions can be implemented for always on cellular devices with a high potential for success that may include positive confirmation from the device that the wipe was completed. However, for WiFi only and on demand cellular devices, incident handling procedures that lock the device out

of accessing CJI may be necessary, while there would be no guarantee that any CJI stored on the device could not eventually be accessed. For this reason, CJI should not generally be stored directly on WiFi only or on-demand cellular devices unless an extremely robust anti-tamper system is in place on the device itself.

Potential device Compromise (software/application)

Incident response scenarios for potential device compromise through intentional or unintentional user action should be developed to ensure compliance with policy. This includes rooting, jailbreaking or malicious application installation on the device during a loss of device control scenario or inappropriate user action in the installation of applications to the device (compromise can occur from either intentional threat agent actions or accidental user actions). Triggers for this incident handling process may be driven from either user notification or electronic detection of device tampering from an audit or MDM compliance check.

Audit and Accountability (CJIS Security Policy Section 5.4)

The ability to implement some Audit and Accountability functions specified in the CJIS Security Policy on mobile devices with limited function operating systems (e.g. Android, Apple iOS) is not natively included within the operating system. Either additional device management systems, enterprise mobility management (EMM) or MDM, or auditing from systems accessed by the mobile device with be necessary to ensure appropriate levels of auditing exist.

Auditable Events (reference 5.4.1)

Some of the specific audit requirements in the CJIS Security Policy may not be technically relevant to the mobile operating system due to its internal functioning. To achieve compliance with the CJIS Security Policy it will be necessary in most cases to utilize some form of MDM or EMM system. Additional auditable events that compensate for the technical limitations of limited function mobile operating systems may be available through the use of MDM systems (e.g. association of event with global positioning system (GPS) location of the device). Specific auditable events of interest in the mobile environment will depend on the intended device usage, compartmentalization of data on the device, and options available with the specific technologies employed. For instance, item 2 in Section 5.4.1.1 indicates an auditable event includes attempts to modify elements of user account modification. Due to the limited internal functions of mobile operating systems, this event type is not relevant to the operating system itself as they are generally provisioned with only a single non-modifiable user account on the device. To achieve compliance in a scenario where CJI is stored or accessed from a secure application on the device, auditing of access to the secure application either through application design, or third party MDM capability may provide an acceptable compensating control. For compliance with the policy each auditable event and event content must be compared to the particular technologies and applications employed to determine if adequate compensating controls are being met for audit items that either do not apply to mobile technologies or cannot be implemented within the technology itself.

Alternative and compensating controls that provide detailed audit of access to CJI either on the mobile device itself or through a controlled application to a central server may provide equivalent auditing capability to the events specified in the policy. However, multiple auditing systems may be required to replicate the auditing provided at the operating system level by a full function operating system. Therefore, the overall auditing design should take into account retrieval and

consolidation of events or audit data from multiple auditing systems as appropriate to comply with policy.

Audit Event Collection

Mobile devices without an 'always-on' cellular connection may pose technical challenges to ensure any audit records collected and stored on the mobile device itself can be retrieved for review and analysis per the CJIS Security Policy. Alternatively systems which explicitly require a network connection to a central server to access data or decrypt on-device storage may provide acceptable audit event collection and reporting since there is a guarantee that network connections must be in pace for CJI to be accessed. Careful consideration should be made regarding the accessibility of audit records when developing the mobile audit scheme.

Access Control (CJIS Policy Section 5.5)

Access control associated to limited functionality mobile operating systems will typically operate in a different manner than full function operating systems. For instance there is normally not a provision for multiple user accounts on many mobile operating systems which may mean the policy requirements for access control (e.g. regarding account management) would not be apply to the mobile operating system, but should rather be applied to a particular application, either stand-alone to the device or as part of a client server architecture. Application of access control policy identified in the CJIS Security Policy will often need to be applied to elements of the total system beyond the device operating system.

For example, CJI stored or accessed from a secure mobile application that requires connectivity to a CJIS authorized server architecture could potentially accomplish most or all of the access control policy elements based on user authorization via the secured application and be largely independent of the mobile operating system. Alternatively, if storing CJI in 'general' purpose data storage containers on a mobile device it may not be possible to achieve compliance with the CJIS Security Policy. Careful consideration and deliberate design of mobile applications or data storage will be required to achieve compliance on mobile devices.

Due to the inherent nature of limited function mobile operating systems, very tight access controls to specific data is actually implemented within the operating system. This effectively prevents applications from accessing or manipulating data associated with other applications to a very high degree of confidence as long as the device is not rooted or jailbroken. However, the device user is automatically granted access to all device data through the associated application unless the application itself has a secondary authentication and access control methodology. Additionally, since basic device functions (e.g. phone) are typically protected using the same password or PIN as the device level encryption, use of a weak PIN to allow easy access to basic device functions largely negates the value of the integrated device encryption.

If personally owned devices are utilized within the environment (BYOD scenario), specialized and costly access control methods may be required to reach compliance with CJIS Security Policy. The costs associated with enhanced access control procedures and technologies should be incorporated in the cost and risk based analysis to determine whether or not to allow personally BYOD, as the technical methods and compensating controls required for CJIS Security Policy compliance are likely to exceed any potential cost savings for implementing BYOD.

Device Control levels and access.

Limited function mobile operating systems are typically very constrained on the levels of access provided to the user. However, intentional user actions (e.g. installing an application and accepting inappropriate security access levels for that application) my bypass some of the built in security protections inherent in the limited functionality devices. Compliance with CJIS Security Policy may be difficult without the addition of strict device control policy. In a mixed environment (e.g. agency owned devices and BYOD), access control policy with BYOD systems may be impractical or impossible to fully implement.

Embedded passwords/login tied to device PIN.

Limited function mobile operating systems typically allow the association of multiple passwords and access credentials with particular applications. The system access provided by these embedded credentials will often be tied to the device password or PIN. An example would be access to device integrated email and calendar applications. Alternatively a 'corporate' email application may independently encrypt the data associated with the application and required a separate login from the device itself. Access to CJI utilizing only the device level password or PIN and device embedded credentials is not compliant with CJIS Security Policy unless protected with Advanced Authentication, which is not currently possible on most devices. Therefore, use of integrated device functions (e.g. built in email or chat) to store or transmit CJI would also not be compliant.

Access requirement specification

In general, due to weaknesses associated with password guessing based on analysis of fingerprints or swipes on the device touch screen, short (4-8 digit) device PIN numbers provide limited security to a determined password guessing attack. Conversely, utilization of a robust password at the device level may be inconsistent with quick access to basic device functions (e.g. phone). When developing specific CJIS compliant access control and authentication schemas a layered approach with the device PIN protecting only the basic device functions (e.g. phone, camera, non-secure applications) and a more robust password or multifactor authentication used to protect applications or data storage may achieve policy compliance where the device password/PIN would not. In a layered security deployment, careful attention must be placed on the capability to share data (e.g. cut and paste or screenshot functions) between secure applications with CJI or CJI access and basic device functions with limited security controls.

Special Login attempt limit

Depending on the access and authentication scheme applied to the mobile device, it may be appropriate to fully comply with the CJIS login attempt limits within a secure application or container and not solely at the device level. However, the device itself should have login attempt limits consistent with the risk associated to the data or configurations accessible on the device itself. Since mobile devices are inherently portable, and can easily be removed from a location. Brute force attempts to gain access to the system, especially when protected only by a short PIN, are likely to be successful given sufficient time. Special consideration should be made based on device connectivity methods (cellular, WiFi, etc) on the appropriate number of unsuccessful login attempts that will be allowed and the resultant actions taken by the device. Most devices either natively allow for the device to wipe itself after a failed number of attempts, or allow the application of EMM/MDM applications to perform wiping actions after a predetermined number of failed login attempts.

Login failure actions

Mobile devices with or without MDM software can typically be configured to perform actions based on serial unsuccessful login attempts. Appropriate actions to configure may be dependent on the data resident on the device and the connectivity method employed by the device. Most devices can be configured to delete all data on the device and/or issue an alert to the network if a number of incorrect passwords are entered. This is a very advantageous feature, however specific configuration of the number of attempts and resultant action must be considered against the state of the device after an unsuccessful attempt action is triggered. A full device wipe will typically leave the device in a fully or partially non-functional state which could introduce risk if part of the intended use is time critical phone calls. Where possible, full device wipe associated with unsuccessful attempts at the device level password should be configured but the number of invalid attempts may exceed the CJIS Security Policy at the device level if all CJI on the device is protected by an additional layer of encryption protected by a subsequent secure application authentication method that is technically prevented (via complexity rules or entry rules) from being the same as the device level authentication and the secure application is configured in accordance with the policy and also contains a secure data wipe capability after a specified number of incorrect authentication attempts.

System use Notification (CJIS Policy reference 5.5.4)

Agency policy should include specific mandatory language consistent with the CJIS Security Policy to identify the device restrictions and consent. However, due to screen size limits, some mobile devices may not be technically capable of displaying the full text used with traditional operating systems. To achieve compliance agencies should contact their legal department for appropriate wording of a short version of the system use notification that can be set to display within the constraints of the device lock screen. This may be accomplished through embedding the text into an image displayed on the lock screen or some other external device labeling method if the device does not permit sufficient text to be displayed.

In a BYOD environment or mixed (agency owned and BYOD), it may be necessary to develop or deploy custom applications that can achieve compliance with the system use notification upon access and prior to any CJI access being allowed.

Session Lock (CJIS Policy reference 5.5.5)

Due to the portable nature of mobile devices the session lock limit in the general CJIS Security Policy may be excessive in the mobile environment for certain device functions and insufficient for other functions based on intended device usage. Agencies should examine the minimum lock time practical for all mobile devices based on their employment scenario and ease for which a user can manually lock the device. The actual session lock times should be adjusted as appropriate to the device type, device operational location, and the data accessible on the device when unlocked. Pocket size devices are at greatest risk if screen lock times are insufficient, however, for devices used in emergency response or communication, extended lock times at the basic device level may be considered if CJI is subsequently protected by an application or web interface utilizing more stringent secure locking functions. A well designed solution may include multiple session lock settings at the device and individual application levels to ensure the CJIS Security Policy requirements are met for CJI access, while other device functions are accessible under different session lock configurations.

Device WiFi Policy

Specific WiFi configuration policy should be developed based on the intended use environment and data access requirements for the device. The policy should explicitly cover configuration of device connections. Technical methods specific to the mobile technologies may need to be implemented to ensure all mobile devices are compliant with CJIS Security Policy. Current CJIS Security Policy provides detailed configuration requirements for WiFi connections, however it was originally intended for defining requirements for fixed infrastructure WiFi (802.11) supporting wireless within a facility. The security requirements identified for fixed infrastructure installations are applicable to mobile usage, however there are several mobile specific scenarios where the requirements may not be clear. The following sections identify areas not specifically covered in the existing policy that will require special handling to ensure wireless connections are compliant.

Hotspot capability

Many mobile devices now include the capability to activate an internal WiFi hotspot that allows other devices to connect through the hosting device to the internet over the devices cellular radio. While this is a potentially valuable capability when multiple law enforcement devices may need localized internet or network access, mobile hotspots should be configured as consistent with the CJIS Security Policy on wireless access points. Connections must only be accepted from known and approved devices in order to protect the integrity of the hosting device as well as the communications security of other connected devices. Since most mobile hotspots are not technically capable of providing the device authentication required for infrastructure wireless, use of mobile hotspot capability should assume the overall portable WiFi network itself is not secure and CJI should not be transmitted or exposed on the network without appropriate encryption.

Connection to public hotspots

There are significant risks to connecting to public wireless access points. Rogue access points masquerading as legitimate public access points may allow for man-in-the-middle, eavesdropping, and session hijacking attacks. While not specifically prohibited in the current CJIS Security Policy, it is recommended that connection to public internet access points be technically restricted by device configuration or MDM systems if possible. CJI access mechanisms from mobile devices should include robust authentication methods specifically designed to prevent interception or hijacking of CJI or user information through the use of a rogue access point masquerading as a legitimate public wireless access point. Transmission encryption alone may not provide sufficient protections when device connections originate at public hotspots. Since the public hotspot controls access to all network services at the connection point (e.g. Domain Name System) attacks against the transmission path are possible that would not normally be feasible in a fixed environment where communications exist between two secured network enclaves.

Cellular Service abroad

If mobile devices are used outside of the United States, especially if connected to foreign cellular networks, specific handling procedures may need to be developed for the use of the device while abroad and the assessment or configuration check of the device state once the devices are returned to the United States. Certain device internal functions on cellular devices may be modified or compromised by the cellular carrier as the devices are intended to have certain parameters configured by the cellular service provider which is considered a ‘trusted’ entity by the device.

Cellular carriers within the United States are constrained by United States laws regarding acceptable modifications to devices. Similar legal constraints cannot be assumed to exist in some areas of the world where laws and regulations for data and personal privacy may allow cellular carriers significantly more leeway in changes made to devices on their networks.

Security plans involving cellular connected devices that will be connected to foreign cellular networks should include technical and policy controls to ensure device use while abroad, data resident on the device while abroad, and the software integrity of the device once returned to the United States are all appropriate to the specific device and threat levels associated with the expected foreign travel. This should explicitly include considerations for devices in which an internal subscriber identity module (SIM) card is inserted into the device to obtain Global System for Mobile (GSM) cellular connections abroad to ensure any residual data on the SIM card is properly purged. Additionally, incident handling procedures may need to specify more stringent responses to even momentary loss of device control, and it may not be possible to assume tracking, anti-theft, and remote data wipe functions that work in the United States would be functional in all potentially visited geographic and political regions.

Bluetooth

Mobile devices utilizing Bluetooth should be evaluated for their ability to comply with the CJIS Security Policy Bluetooth requirements prior to acquisition. This includes the data device itself and any authorized Bluetooth accessories which will be associated to the device. While the technical security in current versions of Bluetooth is significantly stronger than legacy versions, mis-configuration of devices can still pose a significant threat in the mobile environment. If not specifically utilized for a required purpose, it would likely be most cost effective to disable or restrict the device Bluetooth radio utilizing device configurations or an MDM product. Additionally, the using agency may need to develop technically extensive training or user awareness programs to ensure use of Bluetooth capability does not render the device out of compliance if device users have the ability to make Bluetooth associations to the device. Specific instructions or guidance for specific devices could be developed to ensure all implementations are compliant.

Voice/Voice over IP (VoIP)

Cellular voice transmissions are distinctly different at the technical level than Voice over IP (VoIP) transmissions using voice/video applications (e.g. FaceTime, Skype). The use of VoIP is not specifically granted the exemption identified in CJIS Security Policy Section 5.5.7.3.2. Agencies wishing to use capability of this type should ensure the specific technical implementation complies with the Policy on authentication and data encryption.

Chat/Text

Device integrated chat/texting applications and many common third party chat applications authenticate and are identified using embedded passwords or the device identifier only. These functions should not be considered secure or appropriate for transmission of CJI data. Texting functions that utilize a cellular service providers Short Message Service (SMS) or Multimedia Messaging Services (MMS) functions do not constitute a secure transmission medium. Third party applications utilizing appropriate encryption and authentication methods independent of the device password/PIN may provide a compliant solution where the device integrated utilities are will not provide a compliant solution.

Administrative Access

Local administrative access to the mobile device, regardless of device category should be restricted by some mechanism. For traditional operating systems, configuration of a separate administrative account other than that used for normal logins to the device is an acceptable method to ensure appropriate access permissions to the mobile user for which they are authorized. However for limited functionality mobile operating systems (e.g. Android, Apple iOS) internal permissions and accounts assume a single authorized device user with explicitly defined permissions. Those permissions may be modified through policy applied to the device, but are typically global to the device itself. As a result, to ensure appropriate separation of access permissions, it may be required to ensure specific applications or software on the device are configured with individual authentication methods to separate application data from 'general user' access. Without additional authentication at the application level, access to specific application data would be available to any user with the ability to unlock the device. This may be appropriate in some scenarios with a high degree of assurance that the device can only be accessed by a single user, but sufficiently stringent device passwords and short screen lock times may prove problematic for practical use of some device functions. An alternate method to ensure strict separation of 'routine' device functions which may be accessed by multiple individuals (e.g. phone function if loaned to someone for a critical call) is to ensure any method used to access or store CJI has a separate and more stringent authentication method configured with rules that make it impossible to use the same authentication credential (e.g. PIN/Password) on both the device authentication and the application or function with access to CJI.

Rooting/Jailbreaking

'Rooting' (Android OS) or 'Jailbreaking (Apple iOS) refer to intentional modifications to the mobile device operating system in order to grant the device user or an installed application elevated control that would not normally exist on the device. The security model internal to the various mobile device architectures vary significantly, however the common effect of rooting or jailbreaking the devices is to bypass many or all of the built in security features. The security feature bypass may be universal to all device features and installed applications once completed. Intentionally rooting or jailbreaking mobile devices should be avoided in any scenario as it potentially defeats all built-in data access and segregation controls on the device. Additionally the rooting or jailbreaking process itself has a heightened risk of introducing malicious code as part of the process, and also substantially increases the risk for malware to infect the device through user action. Extreme caution should be used if software is being installed that requires the devices to be rooted or jailbroken for the software or application to function. This is inclusive of purported security software that requires a rooted or jailbroken device to function. For example, on both the Android and Apple iOS platforms, the built-in security features for data access and memory segmentation prevent the effective operation of 'traditional' anti-virus and intrusion detection/prevention software. Software or applications purporting to perform these functions but requiring rooting or jailbreaking of the device and may actually accomplish the anti-virus or IDS/IPS function but are also likely to significantly increase the overall risk associated to the device by effectively disabling most or all of the integrated security features. A careful risk-based assessment should be conducted by a trained security professional prior to allowing the operation of any rooted or jailbroken mobile devices regardless of intended use. Significant compensating controls would be required to return a rooted or jailbroken device to minimal compliance with most of the CJIS Security Policy and would likely not be a cost effective approach.

NOTE: There is a distinction between rooting a 'stock' Android installation vice the installation of a separately supported secure operating system. There are secure versions of Android available or that can be developed based on the open source Android source code and compiled for installation on a particular hardware device. Installation of a secure, supported mobile operating system that replaces the device original operating system may significantly enhance the security of the device and should not be confused with 'rooting' and Android installation. Due to the close integration of operating system security with hardware elements, and the proprietary nature of Apple source code, there are not currently separate 'secure' versions of the Apple iOS and it is unlikely they will be developed.

Identity and Authentication

Due to the technical methods used for identity and authentication on many limited functionality mobile operating systems, achieving compliance to CJIS Security Policy may require layering of identification and authentication mechanisms. With the complexity and large number of potential identity and authentication solutions in the mobile environment emphasis must be placed on designing secure identity management and authentication architecture prior to the selection of individual devices or applications. Failure to consider a robust identity and authentication scheme as part of system design or acquisition will significantly increase the risk of subsequent noncompliance with CJIS Security Policy and potential added costs for a remedial solution. Many identity and authentication schemes used by existing commercial applications may make claims that appear to be consistent with CJIS Security Policy Advanced Authentication requirements, however, extreme care must be taken to ensure the actual technical implementation is compliant with policy.

Utilizing Unique device Identification

Some commercial applications and features integrated with some mobile operating systems permit the mobile device to be uniquely identified in a cryptographically robust manner. Any authentication schema that considers the possession of the mobile device as a factor in uniquely identifying and authenticating a CJIS authorized user must also include factors beyond than mere possession of the device. Larger form factor devices that cannot be carried on the person of the authorized user should not rely on possession of the device as an identifying factor, but may still include identifying capability within the device to provide assurance that the device itself is an authorized device. This should still be coupled with multi-factor advanced authentication to the device itself or the application hosting CJI. Coupling unique device authentication with robust advanced authentication of the user provides a high degree of confidence that both the specific device and the operator of the device are correctly identified. Utilizing device unique identification in order to authorize initial connections from the remote device back to the CJI hosting system or enclave provides additional protection to the CJI hosting system to reduce the attack surface of the hosting system and should be considered a good practice, but not in itself an authentication mechanism for the device user.

Certificate Use

One method for uniquely identifying mobile devices is to place part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of identification or authentication in a larger scheme, a certificate alone placed on the device should not be considered valid proof that the device is being operated by an authorized CJIS user, only that the device itself is authorized to host CJIS users. Additional user identification and authentication should be used to supplement any device certificate installed. Using a PIN or password separate from the device login to 'unlock' the certificate from cryptographic storage within a secure application will provide an additional layer of security and may increase the confidence level the device is being used by the intended user. However, use of public/private key pairs or pre-shared encryption keys can be utilized as part of an architecture to protect against certain session hijacking or man-in-the-middle attacks a mobile device may be susceptible to if connected to public internet connections.

Certificate Protections

Any certificates or cryptographic keys stored on any mobile device should include protections against the certificate or key being extracted from the device. Additionally certificates or other keys stored on mobile devices that grant the device special access or unique identification should be configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts. Alternatively, methods may be used to revoke or invalidate the unique certificate or keys associated with a device.

Minimum Password/Pin (Reference CJIS Security Policy Section 5.6.2.1)

The minimum password protections identified in the CJIS Security Policy may not be appropriate for the device PIN/password due to immediate access requirement for some device functions (e.g. phone function) secured by the device PIN/password and the difficulty to enter a complex password under emergency conditions on a small screen. In cases where the risk of a complex password on the device itself is deemed significant, a layered authentication approach may be necessary where CJI or access to CJI is protected via one or more additional layers of access control beyond the device PIN/password. In cases where the CJI or access to the CJI is cryptographically segregated from applications accessible using the device level PIN/Password (e.g. secure application or secure browser vice the built-in browser) the authentication mechanism for the secure application or browser may satisfy the CJIS Security Policy requirements if fully compliant as a stand-alone application.

Configuration Management

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of traditional full-featured operating systems may not function properly on limited function mobile operating systems. Configuration Management systems in the mobile environment may be designed in order to duplicate some of the functions typically performed by traditional anti-malware systems that will not function properly on some mobile operating systems.

Mobile Device Management (MDM)/Enterprise Mobility Management (EMM)

MDM and EMM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented. MDM capabilities include the application of mandatory policy settings on the device, detection of

unauthorized configurations or software/applications, detection of rooting/jailbreaking of the device, and many other security policy related functions. In many cases, the most cost effective way to achieve CJIS Security Policy compliance on mobile devices is the selection of MDM or EMM applications and infrastructure appropriate to the mobile operating systems and intended access to CJI on the mobile devices. MDM/EMM functions may be applicable to most of the CJIS Security Policy requirements and allow for significant compensating controls in areas where traditional methods of CJIS Security Policy compliance are not technically feasible. Section 5.5.7.3.3 of the CJIS Security Policy specifies the minimum functions required for MDM. However, careful selection of the MDM product will potentially provide a cost effective method for additional areas of compliance in the access, auditing, incident response, authentication, media protection and system integrity sections of the CJIS Security Policy.

Device Backups/Images

Device images and backups provide protection against data loss, but also provide a method to quickly recover a device after damage or potential compromise. Due to an inherently limited ability to access the internal file structure of mobile devices, it can be difficult to easily identify a device compromise or illicit modification of the device. Some device imaging and assessment software may provide a secondary forensic capability, especially if there is intent for the device to be used outside the United States.

Bring Your Own device (BYOD) employment

BYOD environments pose significant challenges to the management of secure device configurations. In many cases it may be impossible to apply effective security that is acceptable to the device owner or it may require extremely costly compensating controls to allow access to CJI on personally owned devices. While allowed by the CJIS Security Policy, agencies are advised to conduct a detailed cost analysis of the ancillary costs of compliance with CJIS Security Policy on personally owned devices when they are approved for use. In some cases, a BYOD user may agree to abide by the same device configurations and limitations as imposed on an agency owned device, but signed user agreements should still be in place to ensure the agency has a legal right to recover or clear the device of all data prior to device disposal or employee termination. In other cases, robust secure applications may provide acceptable levels of compliance in a BYOD environment for limited CJI access but application design and architecture should assume the device itself is un-trusted. If MDM/EMM software capable of detecting rooting or jailbreaking of the device is not installed, any CJIS or data access occurring from the device is at a substantially higher risk of compromise.

Configurations and tests

Common configurations specific to all employed mobile devices should be developed to ensure compliance. Configuration tests should be developed and executed on all versions of mobile devices under all possible connectivity scenarios to ensure CJIS Security Policy compliance under all expected operating conditions. Since mobile devices can expect to operate in different physical and network environments, testing and validating correct security functions is more critical than on fixed computing platforms. Additionally, security functions that function properly on one version of a mobile operating system on a particular device may not function in the same manner even on the same version on a different device or a different version on the same device.

Media Protection

Some mobile device hardware platforms include the ability to add removable storage in the form of memory cards. This function is primarily related to Android and Windows mobile platforms and is intentionally limited on Apple devices, but may be possible through certain application functions. While the Android platform performs robust cryptographic separation of data stores between applications within the 'internal' storage of the device, the Android OS does not provide secure separation of data stores on 'external' storage. Some Android hardware devices include additional storage hardwired inside the device that is classified by the operating system as external storage and the normal separation between applications accessing that storage is not applied. Each potential device considered for acquisition must be assessed regarding specific 'external' media protection requirements which may actually include built-in media or storage.

Protection of device connected media

As a result of the limited protection and encryption capabilities applied to device removable media and SIM cards for cellular provisioning that include onboard data storage, all externally removable media or memory should be handled consistently with the CJIS Security Policy on media protection.

Encryption for device media

While most mobile operating systems have the capability to encrypt internal storage, it may require specific device settings to be enabled. All mobile device storage should meet the encryption requirements identified for media in the CJIS Security Policy. Specific settings may need to be applied to ensure proper encryption is actually employed. Additionally, the device built-in encryption capability is typically tied to the device PIN or password. Depending on the device PIN or password requirements the integrated encryption may be easily bypassed by password guessing and appropriate consideration should be made to ensure additional encryption protected by advanced authentication methods be applied to all CJI.

Physical Protection

Due to small form factors and the fact that mobile devices are often stored in lower security areas and vehicles, physical protection of the devices must be considered in both policy and training. Physical protections will often be the responsibility of the assigned device user and physical protections typically inherited by individual information systems from a secure facility will not be available to mobile devices which will require compensating controls to achieve compliance.

Device Tracking/Recovery

MDM software as well as some integrated mobile operating system functions may allow tracking of stolen or lost devices via 'always-on' cellular data connections and the devices built-in GPS. Device tracking with WiFi only or 'on-demand' cellular access may not be reliable. Enabling device tracking capabilities, while not a replacement for secure storage, could be a compensating control used to substantially reduce overall device risk in some scenarios. Device tracking is not currently required in the CJIS Security Policy but should be applied to agency owned devices where possible as a risk mitigation factor. Enabling of device tracking on personally owned devices in a BYOD environment may raise employee privacy concerns and should be considered only for critical systems with the full knowledge of the employee and concurrence of the legal department. This is an enhanced risk that must be accepted for BYOD employments and should be considered

when allowing BYOD employment. Device tracking is available for both limited function mobile operating systems as well as traditional operating systems installed on laptop devices.

Access to device tracking software or applications within the organization should be controlled with limits and formal processes required to initiate a tracking action. It is advisable to include appropriate clauses in user agreements under what conditions and controls the organization applies to device tracking.

Devices utilizing unique device identification/certificates

Devices utilizing unique device identification or have installed certificates may require additional physical protection and/or additional incident handling steps in case of device loss in order to ensure the device unique identifier or certificate is immediately revoked or disabled. Additional physical protection rules or policy would be appropriate for any device which contains access mechanisms tied to the device.

System Integrity (CJIS Policy Section 5.10)

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full-feature operating systems. In many cases the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM or EMM application and supporting server infrastructure.

Patching/Updates

MDM software may provide compliance to the Section 5.10.4.1 patch management requirements for particular platforms and software versions. However, devices without 'always-on' cellular connections may not be reachable for extended periods of time by the MDM or EMM solution either to report status or initiate patching. Supplementary or manual device accountability methods may need to be implemented to account for devices without persistent connections to ensure their patch and update state is current. Alternatively, some patches or system updates may not be practical over cellular connections and will require connection of devices to a WiFi network. Compliance with CJIS Security Policy requirements through purely technical means may not be practical and considerations should be made for aggressive management of devices through training and mandatory periodic connection of devices to organizationally managed WiFi networks.

TECHNOLOGY NOTE: Apple and Android based devices have different potential issues regarding device operating system updates. Apple maintains support for updating the operating system on Apple hardware for several device generations (typically 3-5 years) and provides a robust mechanism for system updates. However, updates to Android based systems are driven by the individual device manufacturer which may or may not support regular updates to current Android operating system versions. Additionally, different Android device vendors may offer updates/upgrades to the Android operating system on different schedules, which can complicate environments utilizing Android devices from multiple manufacturers.

Malicious code protection/Restriction of installed applications and application permissions

MDM or EMM software will typically allow restrictions on installed applications. One of the few effective attack vectors to compromise mobile operating systems is to manipulate the device user to install a malicious application. Even though the application may be restricted from accessing

other application data, it may have some access to common data stores on the device and access to device functions (e.g. GPS, microphone, and camera) that are undesirable. Unrestricted installation of applications by the device user could pose a significant risk to the device.

Malicious code protection using traditional virus scanning software is technically infeasible on most limited function mobile operating systems that are not rooted or jailbroken. The integrated data and program separations prevent any third party installed program from accessing or 'scanning' within another application data container. Even if feasible, power and storage limitations would be prohibitive in the effect on device battery life and storage capacity on most mobile devices. However, the cryptographic separation between applications and effective application virtualization technologies built into common mobile operating systems partially compensate for the lack of traditional virus scanning technologies. Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a matter analogous to traditional virus scan detection of unauthorized software. This behavior is analogous to the software inventory performed by anti-virus products and can provide a high degree of confidence that only known software or applications are installed on the device. While it is theoretically possible to bypass the application sandboxing and data segregation protections to compromise a mobile device through the web browser, the attack methods required are significantly more advanced than those required for a traditional full-featured operating system. Malicious code protections on the device web browser can be enforced through the use of a properly protected web proxy which the device is configured to use as a mandatory device policy. The most common method of malicious code installation is enticing the user to manually install the malicious app which can be mitigated on organizational devices using an MDM or other application installation restrictions which prevent the user from installing unauthorized or unknown applications. Mitigation of this issue within BYOD environments may not be possible and will present a significantly enhanced risk to the device.

TECHNOLOGY NOTE: In the particular area of application installation there is a significant difference between the behavior of Apple iOS and Android platforms. Apple cryptographically restricts the way applications will execute on the device and assigns mandatory application permissions when the application code is signed prior to release on the Apple App Store for distribution. Apps on the Apple platform must conform to Apple's policy on app behavior and cannot exceed their design permissions on access to common device functions once the app has been signed and distributed. However, the Apple method does not typically advertise the precise internal permissions granted to the app to the user prior to installation. At runtime, the app is required to request user permission to access certain device functions, and the user may agree or not agree, which may introduce risk if they are unaware of what they are agreeing to allow. Unsigned or un-trusted apps are cryptographically prevented from executing on non-jailbroken iOS devices. Apple provides a mechanism for organizations to distribute custom apps within an organization with equivalent protections but all receiving devices must have a special certificate installed that will only allow official App Store and the organization custom apps to execute.

Conversely, the Android platform, while also requiring app code signing, allows for self-signed code which can be distributed be means other than an official app store and execute on any Android device. Application permissions are presented to the user once at app installation but ramifications of agreement to certain app permissions may not be obvious to a non-technical user. Permissions in the Android model require user acceptance of all app requested permissions or the app is denied

installation, which can result in unwise user acceptance of excessive permissions in order to gain functionality provided by the app.

On either platform user installation of applications can significantly change the security state of the device. Applications may be able to transmit and receive data or share device common data with other devices over the network or local WiFi or Bluetooth connection. On either platform it is highly desirable to limit allowable applications to a pre-approved pool of apps via MDM or organizational App store structures and device policy. However, the risks associated with uncontrolled app installation is several orders of magnitude greater on Android based devices.

WARNING: Rooted or jailbroken devices are modified in such a manner that the built in protections against malicious code are effectively disabled. A rooted or jailbroken device would require significant and costly compensating controls to achieve compliance.

Firewall/IDS capability

Traditional device or "personal' firewalls as identified in CJIS Security Policy Section 5.10.4.4 may not be practical on limited function mobile device operating systems but significant compensating controls are available. By default, mobile device operating systems have a limited number of system services installed and carefully controlled network access. To a certain extent the mobile operating system performs similar effective functions as a personal firewall would perform on a general purpose operating system. Potential compensating controls for the five (5) personal firewall requirements specified in Section 5.10.4.4 are listed below:

1. Manage Program Access to the Internet: On agency controlled devices with an MDM, limiting the apps installed on the device will effectively perform the same function. Since no software or apps can be installed without MDM approval a robust approval process can effectively ensure internet access is only granted to approved apps. Built-in apps and functions can also be limited on network access by the MDM.
2. Block unsolicited requests to connect to the user device: Default configurations for mobile operating system platforms typically block incoming requests. It is possible to install an app that may 'listen' on the network and accept connections, but the same compensating control identified in item 1 will mitigate the likelihood of that occurring.
3. Filter incoming traffic by IP address or protocol: Protocol filtering effectively occurs due to the limited function of the operating sys long as no installed application opens network access ports. The mitigations in 1 effectively compensate for this control as well.
4. Filter incoming traffic by destination ports: Same as 3.
5. Maintain an IP traffic log: This may not be technically feasible on most mobile operating system platforms as maintaining this log would require access to lower level operating system functions that are not accessible unless the device is rooted or jailbroken. However, individual Apps that communicate over the network or accept connections from the network may permit logs of IP traffic associated to that application to be stored.

Spam Protection

Spam guards installed on corporate or organizational email systems may effectively accomplish the spam protection requirements for the CJIS Security Policy on mobile devices if properly configured to block spam before delivery to the device. If no upstream spam guard is installed on the mail server the mobile devices accesses, the device may not have adequate spam protection. Additionally access to internet based email (web mail) would need to be restricted to web mail with appropriate spam and/or antivirus protections to ensure compliance.

Periodic system integrity checks

One method to compensate for the technical infeasibility of traditional anti-virus and malicious code protection is to install an MDM that performs periodic system integrity checks that validate device configuration and status against an approved baseline. Deviations may provide indicators of potential device compromise or mis-configuration.

G.5 Administrator Accounts for Least Privilege and Separation of Duties

Administrator Accounts for Least Privilege and Separation of Duties

PURPOSE:

This appendix is provided to describe industry best security practices for assigning separate administrator accounts to support the concept of Least Privilege.

ATTRIBUTION:

- SANS, "The Critical Security Controls for Effective Cyber Defense", version 5.0
- NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations", Revision 4 dated April 2013
- NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook" dated October 1995
- CNSSI-4009, "National Information Assurance (IA) Glossary", dated April 2010

DEFINITIONS:

Least Privilege – The principle that security architecture be designed to grant individual users and processes only the minimum accesses to system resources and authorizations required to perform their official duties or function.

Separation of Duties – The security principle requiring the division of roles and responsibilities so that a single individual cannot subvert a critical process or function.

SUMMARY:

The implementation of least privilege is accomplished by assigning user or process access to system resources based on operational or business needs. Thus, access is granted to only those resources required to perform assigned duties. For individuals who have multiple roles within the organization requiring varying levels privileges, this assignment of access can be challenging. Often times the agency will assign a single userid to the individual and elevate the privileges for that account based on the different roles. While it may seem logical to allow the user access to all

required resources using a single account, security vulnerabilities can be introduced into the system.

Associated with least privilege is separation of duties. This concept aids in maintaining the integrity of the system by preventing the abuse of elevated privileges for making unauthorized changes to the system. This objective essentially requires different individuals to perform separate functions with relation to (primarily) administrative duties. For instance, those with the ability to create and assign user access to system should not be able to access the audit logs that contain the evidence of the account actions.

USER ACCESS AND ACCOUNT MANAGEMENT:

Several factors influence the manner in which an agency implements and manages user access. Many times, the size of the agency and the technical expertise of the IT staff employed by the agency become primary drivers. Larger agencies with a broad base of technically savvy personnel normally have the ability to dedicate resources specifically to the administration and management of user access. This could translate to the use of multiple accounts for a single user performing duties requiring varying levels of access.

Smaller agencies with few or no technically experienced personnel will often assign single user accounts with the highest level of access required by users. Other smaller agencies may go as far as assigning every user an account with elevated privileges so there are no delays or problems requiring intervention by already overburdened system administrators. It is not uncommon for a smaller agency to outsource system administration duties.

Regardless of the size or resources of an organization, each agency should base the process for assigning access to system resources based on their operational requirements and a thorough risk assessment. To mitigate risk for accessing system resources, industry best security practices prescribe those individuals performing duties requiring elevated privileges be assigned a separate userid to be used in the performance of those duties. This account would be separate from a standard user account.

Why are some agencies unwilling to implement controls for least privilege? One common reason/perception is administrative overhead. There is a time factor for a system administrator to create user accounts and configure those accounts correctly based on the user's role. In larger agencies with many employees, this could add up to a significant impact on the system administrator(s) especially if there is a high level of turnover. Resources in some agencies may allow for a single system administrator dedicated strictly for account management. On the other end of the spectrum, in agencies with fewer employees, the impact may be more burdensome. While there are fewer user accounts to manage, a full-time system administrator for account

management may not be feasible. Those duties then become shared between a few people or added to the duties of a lone person.

Another reason may be the burden on system administrators to remember multiple userids and passwords. This could result in the user using the same password for each account or the user writing down the credentials for ease of remembrance. Additionally, an administrator could get the credentials mixed up between accounts causing an account lockout. This could then require system administrator intervention to reset or unlock the account.

Some agencies may feel that creating additional accounts reduces system resources. Depending on the size of the agency, this could be a concern. In most cases, the number of individuals that would require a secondary account would be minimal. The impact could be limited to a slight increase in disk space usage on the systems accessed by the system administrators with the separate accounts and perhaps the server housing the account information.

THREATS:

A primary goal of attackers is to gain administrative or root privileges on a network or system. Therefore, protection of credentials with that level of access is a key to preventing unauthorized access. Attackers may use many methods in attempts to gain unauthorized, privileged access to computer or network systems. There are two common techniques that take advantage of improperly managed administrative privileges.

Phishing Attacks

In this first method, consider a small organization with limited system administrative resources. Each user is assigned an account with elevated privileges that allows them to perform a myriad of duties including gaining access to critical system security resources. Because this is the only account the user has, normal non-administrative duties are also performed with administrative rights. While checking their email, the user is fooled into reading a message and opening a malicious attachment. Because the user's account has elevated privileges, malware is now installed on the system with elevated privileges. The malware could now allow the attacker to take over the system and install other malicious software such as key loggers, sniffers, or remote control applications. Other key system resources such as firewalls, routers, switches, or intrusion detection systems are now also compromised.

Password Brute Force Guessing / Cracking

The second method may not be as easy as the first and involves the guessing or cracking of passwords on the part of the attacker. Based on human nature, we tend to develop passwords that

are easy to remember and most likely contain some kind of information that is pertinent to us. Some passwords could be easily guessed with a minimal amount of social engineering or fact finding. Consider again an agency that assigns users a single account to perform all duties including those requiring elevated privileges. A user has created a password that, while meeting the requirements of the CJIS Security Policy, is comprised of easily guessed information about the user. An attacker has previously determined the userid and is now able to begin guessing the password. Upon success, the attacker will have unauthorized access to critical system resources.

MITIGATION:

The first step to implementing least privilege is to create separate user accounts for those individuals that require elevated privileges for their duties. These duties could include system or security administration, reviewing audit logs, backup administration, or configuring network devices (e.g. firewalls, routers). The passwords associated with these accounts should have a higher level of complexity than an account without elevated privileges. By disassociating the access levels required for system administration functions from an individual's "everyday use account", should a password be compromised, access would be limited to that of a user with non-elevated privileges.

Second is to implement procedures to ensure accounts with elevated privileges are used only for those duties requiring the higher level of access. This would mean disabling or blocking access to email, web browsers, and other external facing connections. While technical processes are the preferred method of preventing the misuse of accounts with elevated privileges, written policies can be used in situations where technology does not support that type of account management.

Several governance organizations recognize the importance of the security value of Least Privilege. The Payment Card Industry (PCI) includes requirements in their Data Security Standards (DSS). The National Institute of Standards and Technology (NIST) addresses the concept of Least Privilege in its Special Publication (SP) 800-53 rev. 4. While not considered a governance organization, the System Administration, Networking, and Security (SANS) Institute publishes a list of the top 20 security controls which includes "Controlled Use of Administrator Privileges" at number 12. Although the actual security controls or required implementation may slightly differ, the concept is consistent across the groups. The actual controls from NIST and SANS are included here in this appendix.

NIST CONSIDERATIONS FOR LEAST PRIVILEGE:

NIST Special Publication 800-53 rev. 4 includes controls required for all systems under the Federal Information Security Management Act. The publication specifies the guidance for Least Privilege in the control catalog under the Access Control (AC) family and specifically as AC-6. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of

the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-6 is a key control having several enhancements which, when implemented, bolster the overall security of the information system by reducing the risk of compromise through the misuse or misconfiguration of access to system resources.

AC-6 Least Privilege

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

Control Enhancements:

(1) *LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*

The organization explicitly authorizes access to [*Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information*].

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.

Control Enhancements:

(2) *LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*

The organization requires that users of information system accounts, or roles, with access to [*Assignment: organization-defined security functions or security-relevant information*], use non-privileged accounts or roles, when accessing nonsecurity functions.

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.

(3) *LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*

The organization authorizes network access to [*Assignment: organization-defined privileged commands*] only for [*Assignment: organization-defined compelling operational needs*] and documents the rationale for such access in the security plan for the information system.

Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.

(4) *LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS*

The information system provides separate processing domains to enable finer-grained allocation of user privileges.

Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example: (i) using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; (ii) employing hardware and/or software domain separation mechanisms; and (iii) implementing separate physical domains. Related controls: AC-4, SC-3, SC-30, SC-32.

(5) *LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*

The organization restricts privileged accounts on the information system to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.

(6) *LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS*

The organization prohibits privileged access to the information system by non-organizational users.

Supplemental Guidance: Related control: IA-8.

(7) *LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES*

The organization:

(a) Reviews [*Assignment: organization-defined frequency*] the privileges assigned to [*Assignment: organization-defined roles or classes of users*] to validate the need for such privileges; and

(b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.

(8) *LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION*

The information system prevents [*Assignment: organization-defined software*] from executing at higher privilege levels than users executing the software.

Supplemental Guidance: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such

applications/programs, those users are indirectly provided with greater privileges than assigned by organizations.

(9) *LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*

The information system audits the execution of privileged functions.

Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Related control: AU-2.

(10) *LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** AC-6 (1) (2) (5) (9) (10)	**HIGH** AC-6 (1) (2) (3) (5) (9) (10)

SYSTEM ADMINISTRATION, NETWORKING, AND SECURITY (SANS) CONSIDERATION FOR LEAST PRIVILEGE:

There are many negative factors that affect our cyber lives: massive data loss, intellectual property theft, credit card breaches, and identity theft just to name a few. Cyber defense is rapidly evolving to address the plethora of challenges we face. Defenders have access to a wide array of resources to combat those wishing to do harm. Ranging from the collection of vast amounts of intelligence data to security standards to training and certifications, security practitioners are well armed.

But can information overload actually worsen the problem? Organizations must decide, hopefully based on risk analysis, how to wade through all available resources and select those best suited to their own operating environment. The threats continue to evolve, the attackers become smarter, and user access more mobile. The cloud beckons and can provide reduced cost and infrastructure at a price of less control and accountability for vital information.

The SANS Institute publishes the "20 Critical Security Controls for Effective Cyber Defense". This list of controls is the combined result of work by an international community to create, adopt, and support the controls. The components of the community provide insight, tools, information, and solutions into threats and adversaries. This list includes the control titled "Controlled Use of Administrative Privileges". SANS describes this control as: *The process and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

Critical Security Control (CSC) 12: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

ID #	Description	Category
CSC 12---1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	*Quick win (One of the "First Five")*
CSC 12---2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.	*Quick win*
CSC 12---3	Configure all administrative passwords to be complex and contain letters, numbers, and special characters intermixed, and with no dictionary words present in the password. Pass phrases containing multiple dictionary words, along with special characters, are acceptable if they are of a reasonable length.	*Quick win*

CSC 12---4	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration---level accounts.	*Quick win*
CSC 12---5	Ensure that all service accounts have long and difficult--- to---guess passwords that are changed on a periodic basis, as is done for traditional user and administrative passwords.	*Quick win*
CSC 12---6	Passwords should be hashed or encrypted in storage. Passwords that are hashed should be salted and follow guidance provided in NIST SP 800---132 or similar guidance. Files containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with super---user privileges.	*Quick win*
CSC 12---7	Utilize access control lists to ensure that administrative accounts are used only for system administration activities, and not for reading e---mail, composing documents, or surfing the Internet. Web browsers and e---mail clients especially must be configured to never run as administrator.	*Quick win*
CSC 12---8	Through policy and user awareness, require that administrators establish unique, different passwords for their administrative and non---administrative accounts. Each person requiring administrative access should be given his/her own separate account. Users should only use the Windows "administrator" or UNIX "root" accounts in emergency situations. Domain administration accounts should be used when required for system administration instead of local administrative accounts.	*Quick win*
CSC 12---9	Configure operating systems so that passwords cannot be re---used within a timeframe of six months.	*Quick win*
CSC 12---10	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.	*Visibility/ Attribution*
CSC 12---11	Configure systems to issue a log entry and alert when unsuccessful login to an administrative account is attempted.	*Visibility/ Attribution*

CSC 12---12	Use multifactor authentication for all administrative access, including domain administrative access. Multi--- factor authentication can include a variety of techniques, to include the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics.	*Configuration/ Hygiene*
CSC 12---13 (NEW)	When using certificates to enable multi---factor certificate---based authentication, ensure that the private keys are protected using strong passwords or are stored in trusted, secure hardware tokens.	*Configuration/ Hygiene*
CSC 12---14	Block access to a machine (either remotely or locally) for administrator---level accounts. Instead, administrators should be required to access a system using a fully logged and non---administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems. Users would use their own administrative accounts and enter a password each time that is different than their user account.	*Configuration/ Hygiene*

Quick win: Implementation provides significant risk reduction without major financial, procedural, architectural, or technical changes to an environment, or that provide substantial and immediate risk reduction against very common attacks that most security-aware organizations prioritize these key controls.

Visibility / attribution: Measures to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.

Configuration / hygiene: reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.

SEPARATION OF DUTIES:

Separation of duties is another security control related to least privilege. Many of the same challenges faced by least privilege apply to this concept as well. Agency size and resources play a major in the implementation of separation of duties. As the name implies, some key functions should be separated between different individuals. The goal of this concept is to provide protection

against a single individual's ability to circumvent system security controls to gain unauthorized access or perform unauthorized actions without colluding with other individuals.

Simply put separation of duties entails distributing certain critical mission oriented functions or system administrative support functions amongst different individuals or roles. It also includes delineating information system support duties such as auditing, configuration control, or network security between different individuals.

As with least privilege, an agency's ability to implement separation of duties is typically based on financial and personnel resources. While a very large agency may have ready availability to those resources to ensure critical functions are spread across multiple individuals, a small agency probably does not have that luxury.

THREATS:

What effect can an individual with carte blanc access to all critical functions of a system have? Consider a single individual with the ability to install nefarious applications on a system (e.g. a keylogger). If this same individual also has the ability to edit any audit logs that would have recorded the actions of installing the software, those entries could be deleted and any evidence of the installation eliminated.

Perhaps a disgruntled system administrator wants to open a port on a firewall to allow a remote backdoor connection into the information system in order to siphon off criminal justice information. Because the perpetrator has access to the firewall and all logs, the port can be opened and the logs tampered with to eliminate records of the action.

As mentioned previously, the two concepts of least privilege and separation of duties are related. Additional threats are presented when a system administrator using a single account with unlimited elevated privileges across the information system uses that account to check email. In a successful phishing attack that compromises this account, the attacker now has unrestricted unauthorized access to all system resources and the ability to hide their tracks.

MITIGATION:

The primary method to avoid these situations is to configure system privileges and duties such that a single person is unable to effect questionable change to the system and then are able to erase any evidence of the change.

Technical configurations are most secure and sound enforceable policies compliment the technical solutions. When an information system does not support separating duties, strong policies help mitigate risk.

NIST CONSIDERATIONS FOR SEPARATION OF DUTIES:

NIST Special Publication 800-53 specifies the guidance for separation of duties in the control catalog under the Access Control (AC) family and specifically as AC-5. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-5 is a relatively small control with no enhancements but it is significant in protecting the integrity of an information system.

AC-5 Separation of Duties

Control: The organization:

a. Separates [*Assignment: organization-defined duties of individuals*];

b. Documents separation of duties of individuals; and

c. Defines information system access authorizations to support separation of duties.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-5	HIGH AC-5

G.6 Encryption

Encryption

Purpose:

This paper was created to provide assistance and guidance on encryption types, methods, and to provide general best practices in the implementation of encryption.

Attribution:

- FIPS 140 – 2, Security Requirements for Cryptographic Modules (May 2001)
- FIPS 197, Advanced Encryption Standard (Nov 2001)
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
- CNSSP-15, National Information Assurance Policy on the Use of Public Standards for Secure Sharing of Information among Security Systems
- CJIS Security Policy

Definitions and Terms:

Encryption – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Decryption – The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Asymmetric Encryption **–** A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Symmetric Encryption **–** A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption**.**

Hybrid encryption – A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality**.**

Authorized User/Personnel - An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Summary:

CJIS Security Policy encryption requirements are intended to provide protection of the sensitive data that is criminal justice information (CJI). The primary goal of encrypting CJI is to prevent unauthorized access to this sensitive data. Encryption is a great tool that can be applied to accomplish this protection and ensure compliance with the vast majority of the CJI requirements. CJIS Security Policy Section 5.10.1.2 details when encryption is required and provides information on the exceptions to the encryption requirement.

Achieving CJIS Security Policy Compliance:

To determine when encryption is required one must first read and understand CJIS Security Policy Section 5.9.1 Physically Secure Location. The reason for this is simple: encryption is not required while within a physically secure location. Conversely, whenever CJI is transmitted or stored (at rest) outside the boundaries of a physically secure location encryption may be required. The exact standards to which the data would be required to meet are detailed along with any exceptions in CJIS Security Policy Section 5.10.1.2.

Additionally, both security awareness training and personnel security requirements can be affected by whether or not CJI is encrypted. Requirements surrounding these Policy areas is determined by answering the following question: Who has unescorted access to unencrypted CJI?

Unless personnel is escorted, security awareness training is required as correlated with the access level needed by personnel as identified in CJIS Security Policy Section 5.2. Similarly, fingerprint-based background checks as detailed in CJIS Security Policy Section 5.12 may be required on individuals to permit unescorted access to CJI.

The intent of all these requirements is to limit access to CJI to only authorized personnel. CJIS Security Policy Appendix A: Terms and Definitions defines authorized user/personnel as an individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

What is Encryption?

Encryption is the process of encoding messages or information in such a manner that only people with the knowledge or means to decrypt the message can do so. But how does this work?

In an encryption process, legible data, referred to as plaintext, is encrypted by applying a cipher (otherwise known as an encryption algorithm or crypto key) to the data. The data then becomes encrypted and is now referred to as ciphertext. The ciphertext is essentially unreadable until decrypted. The decryption process requires the process of applying the same algorithm (crypto key) to encrypt the data in an inverse manner to convert the data back into plaintext.

Encryption is important because it allows you to securely protect data that you don't want anyone else to have access to. Encryption has been used throughout history to send “secrets” securely by some form of obfuscation to a recipient. Businesses and enterprises use encryption to protect corporate secrets and sensitive employee data, such as payroll information and personally identifiable information (PII). Governments secure classified information with encryption. Additionally, individuals may use encryption to protect personal information, such as credit card data, banking information, and passwords to guard against things like identity theft.

It should be known that encryption may not always prevent the interception of data. If the stolen data is encrypted, though, it would be extremely difficult for any of the data to be decrypted without having the decryption key. While it may be possible to decrypt the message without possessing the key, it does require large computational resources, great skill, and lots of time to accomplish such a task. Exercising encryption along with key management policies is one of the best security practices that can be put into place with regard to sensitive data security and protection.

Types of Encryption:

<u>Symmetric Encryption</u>

Symmetric encryption is also commonly known as secret key encryption. Symmetric encryption is a form of cryptography utilizing a singular encryption key to guise an electronic message. Its data conversion uses a mathematical algorithm along with a secret key, which results in the inability to make sense out of a message. Symmetric encryption is a two-way algorithm because the mathematical algorithm is reversed when decrypting the message along with using the same secret key.

Symmetric encryption is most often used for data protection whether at rest or in transit, especially in bulk, due to the ease and speed with which the encryption can be implemented. The most common examples of symmetric algorithms are: AES and Triple-DES (3DES or TDEA).

How it works:

To encrypt and send a message to Jane, John does the following:

1. Generates a new symmetric key
2. Encrypts the message using this new symmetric key
3. Sends the message to Jane
4. Sends the encrypted symmetric key to Jane - out of band

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Receives the symmetric key
3. Uses the symmetric key to decrypt the message

Asymmetric Encryption

Asymmetric encryption is also commonly known as public-key encryption Asymmetric cryptography is cryptography in which a pair of keys, a public key and a private key, are used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

Creating Key Pairs:

Asymmetric encryption requires the use of algorithms of great computational complexity to create the key pairs. This is accomplished by using a large, random number that an algorithm is applied to which generates a pair of keys for use as asymmetric key algorithms (as shown in Figure 1 below).

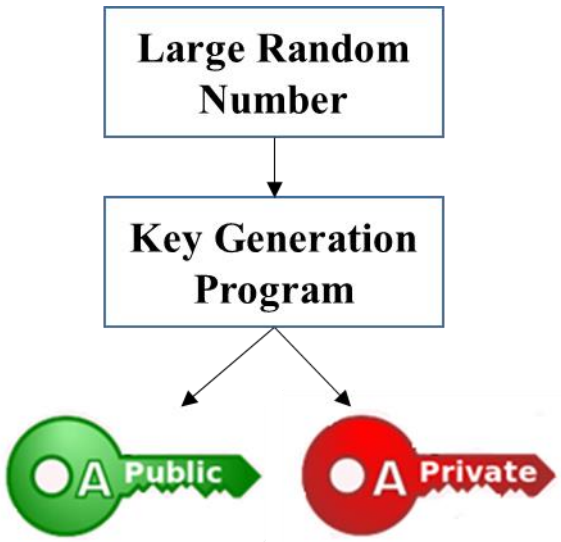


Figure 1 – Asymmetric key pair generation

Asymmetric encryption is most often used to encrypt a single message before transmission. The most common examples of asymmetric algorithms are: RSA and DSA.

How it works:

To encrypt and send a message to Jane, John does the following:

1. Obtains Jane's public key
2. Encrypts the message using Jane's public key
3. Sends the message to Jane

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Uses her private key to decrypt the message

Advantages of Using Symmetric Encryption for Data Protection

Asymmetric encryption requires the use of algorithms with great computational complexity to create the key pairs, and therefore is not practical for large amounts of data. It is typically used for only for short messages. Also, asymmetric encryption must use a comparatively stronger key than symmetric key encryption to achieve the same level of protection as one key (public) will be published in the public directory for all to see.

Symmetric encryption is based on large, but simple algorithms which require less computation. Therefore, is much faster to create and use keys. This allows the same key to be used to encrypt and decrypt the message. So, data can be encrypted in real time. The (shared) key is sent to the recipient out of band so that it can be used to decrypt the data.

For the reasons stated above, symmetric key encryption is the preferred choice by both industry and government alike to encrypt large amounts of data (bulk encryption) simply due to the ease and real time encryption capabilities as detailed above. Additionally, a new key can be generated for every session, message transaction, etc., as desired. This means a sender won't have to use one key (public) to encrypt a message and have the recipient use another key (private) to decrypt the message.

Hybrid Encryption

Hybrid encryption solution exist where both asymmetric encryption and symmetric encryption keys are used to create what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality**.**

Hybrid solutions are most often used by Internet browsers to protect data in transit. The most common examples of hybrid encryption are: TLS/SSL, PGP, IPSEC, and S/MIME.

How it works:

To encrypt a message to Jane in a hybrid cryptosystem, John does the following:

1. Obtains Jane's public key
2. Generates a new symmetric key
3. Encrypts the message using this new symmetric key
4. Encrypts the symmetric key using Jane's public key
5. Sends the message to Jane

To decrypt this hybrid cipher text, Jane does the following:

1. Receives the encrypted message
2. Receives the encrypted symmetric key
3. Uses her private key to decrypt the symmetric key
4. Uses the symmetric key to decrypt the message

Explaining Cipher Suites:

A cipher suite is a set of cryptographic algorithms used for the following:

- Protect information required to create shared keys (key exchange)
- Encrypt messages exchanged between clients and servers (bulk encryption)
- Generate message hashes and signatures to ensure the integrity of a message (message authentication)

Examples of Transport Layer Security (TLS) 1.2 Cipher Suites:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

A cipher suite specifies one algorithm for each of the above tasks. For example, the TLS_RSA_WITH_AES_128_SHA256 cipher suite is used for TLS. The suite uses the RSA asymmetric algorithm for key exchange, AES with a 128-bit key for bulk data encryption, and SHA256 for message authentication.

Symmetric and Asymmetric Key Strength Comparison:

Symmetric		**Asymmetric**		
Bits of security	**Symmetric key algorithms**	**Finite-Field Cryptography (FFC) (e.g., DSA, D-H)** **Bits of security**	**Integer-Factorization Cryptography (IFC) (e.g., RSA)** **Bits of security**	**Elliptic-Curve Cryptography (ECC) (e.g., ECDSA)** **Bits of security**
80	2TDEA18	*Public key* = 1024 *Private key* = 160	*Key size* = 1024	*Key size* = 160-223
112	3TDEA	*Public key* = 2048 *Private key* = 224	*Key size* = 2048	*Key size* = 224-255
128	AES-128	*Public Key* = 3072 *Private key* = 256	*Key size* = 3072	*Key size* = 256-383
192	AES-192	*Public key* = 7680 *Private key* = 384	*Key size* = 7680	*Key size* = 384-511
256	AES-256	*Public key* = 15360 *Private key* = 512	*Key size* = 15360	*Key size* = 512+

Figure 2 - Symmetric and asymmetric key strength comparison

As you can see in the chart provided above, the equivalent key strengths between symmetric and asymmetric key strengths do not necessarily correlate. There is a reason for this. As stated previously, asymmetric algorithms must use a comparatively stronger key than symmetric key encryption to achieve the same strength. The simplest explanation for this is because one of the keys is published to the public directory and can constantly be attacked by anyone with access to the directory. Therefore, the public key must be made of such strength that it can resist getting compromised while made public.

Federal Information Processing Standard (FIPS) 140-2 Explained

Origin of FIPS 140-2

On July 17, 1995, the National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) to validate cryptographic modules to Federal Information Processing Standards (FIPS) Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment Canada (CSEC). FIPS 140-2, Security Requirements for Cryptographic Modules, was released on May 25, 2001 to supersede the original FIPS 140-1. Modules validated as conforming to FIPS 140-1 and FIPS 140-2 are accepted by the Federal Agencies of both countries for the protection of sensitive information.

What is FIPS 140-2?

Federal Information Processing Standard (FIPS) is a standard developed and recommended (often mandated) for use in federal-government-operated IT systems by the following two government bodies:

- The National Institute of Standards and Technology (NIST) in the United States
- The Communications Security Establishment (CSE) in Canada

FIPS 140-2 specifies the security requirements a cryptographic module must meet when utilized within a security system protecting sensitive information within information systems (computer and telecommunication systems). FIPS 140-2 specifies which encryption algorithms can be used and how encryption keys are to be generated and managed.

How does a product get certified?

Vendors of cryptographic modules can have their products tested by independent, accredited Cryptographic and Security Testing (CST) laboratories. The CST laboratories use the Derived Test

Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules against the applicable standards in a variety of implementations. The result of these tests are reported to NIST's Computer Security Division (CSD) and CSEC who jointly serve as the Validation Authorities for the program. These results are then reviewed and certificates would be issued if the results are determined to be acceptable.

What is the difference between being FIPS 140-2 compliant and being FIPS 140-2 certified?

It is common theme to discover a product is “FIPS compliant.” What does this mean, though? The difference between compliance and certification is not subtle. Certification requires a vast testing, verification, and validation process be performed by a CST laboratory as described in the previous section. Compliance is merely a claim stating the implementation of an encryption solution is done in accordance with the security policy related to the FIPS certification. Any claim of compliance would need to be validated and the corresponding certificate number would have to be known.

NIST has addressed related claims as shown below in their Frequently Asked Questions for the Cryptographic Module Validation Program:

> A vendor makes the following claims of conformance to FIPS 140-2. Are they acceptable?
>
> • The module has been designed for compliance to FIPS 140-2. <NO>
>
> • Module has been pre-validated and is on the CMVP pre-validation list. <NO>
>
> • The module will be submitted for testing. <NO>
>
> • The module has been independently reviewed and tested to comply with FIPS 140-2. <NO>
>
> • The module meets all the requirements of FIPS 140-2. <NO>
>
> • The module implements FIPS Approved algorithms; including having algorithm certificates. <NO>
>
> • The module follows the guidelines detailed in FIPS 140-2. <NO>
>
> • The module has been validated and has received Certificate #XXXX. <YES>
>
> A cryptographic module does not meet the requirements or conform to the FIPS 140-2 standard unless a reference can be made to the validation certificate number. The module used must also be the same version/part number as annotated on the validation certificate. Any other claims are not relevant.

To read more FAQs from NIST on FIPS certification, use the following NIST website link: http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPFAQ.pdf

Where can I learn more about FIPS 140-2?

For more information about the FIPS 140-2 standard, go to the following NIST website: http://csrc.nist.gov/cryptval/140-2.htm

General Recommendations:

Encryption key management control is of paramount importance! Agencies should develop policies and procedures define and monitor the administrative tasks involved with protection, storage, organization, access controls and the lifecycle management of encryption keys. After all, encryption keys should not be accessible by just anyone. An encryption key management control process should ensure only authorized users have access to encryption keys. Key management is a best security practice and helps to ensure the confidentiality and integrity of CJI data and enforces key access control.

The CJIS Security Policy is a "living" document under constant review and receiving regular updates through the Advisory Policy Board (APB) process. Agencies need to always keep up to date on the latest requirements. These requirements can be found in CJIS Security Policy Section 5.10.1.2. Please contact the CJIS ISO Program anytime to address any questions or concerns about CJIS Security Policy requirements, the current APB status of CJIS Security Policy requirements, or if seeking general information or guidance.

G.7 Incident Response

Incident Response

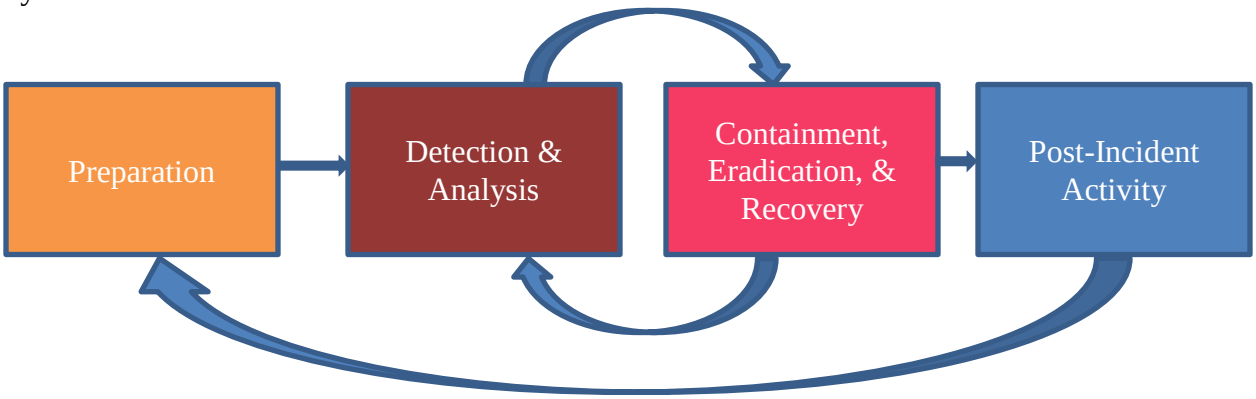
Introduction

Information technology (IT) security incident response is an important and critical component of information technology programs. Performing incident response effectively can be a complex undertaking – for that reason, establishing a successful incident response capability requires planning and resources. Everyone in an organization must be aware of IT security risks, threats, and actions to take in situations where an actual IT security incident has occurred. Even the best-secured and controlled environments can experience these security risks, threats, events, and incidents. This document provides guidelines for appropriate response to IT security incidents, and are independent of specific hardware platforms, operating systems, protocols, or applications.

The following example incidents are used to highlight appropriate actions during each phase:

- Malicious code execution
- Ransomware execution
- Denial of service attack
- Social Engineering
- Phishing

NIST Special Publication 800-61 rev. 2 outlines the "Incident Response Life Cycle" as a collection of phases – distinct sets of activities that will assist in the handling of a computer security incident, from start to finish. The following diagram explains the process flow of the incident response life cycle:



Preparation

The initial phase of the incident response life cycle, "Preparation", involves establishing and training an incident response team, and acquiring the necessary tools and resources. A computer security incident may not have happened at this phase, but it is important to utilize all available knowledge and security measures to obtain the best posture for responding to potential future incidents. One of the most important preparation steps involves the collection, storage, and accessibility of event data and telemetry from hardware and software resources such as firewall logs, application logs, operating system logs, and other valuable sources of situational data, as well as the output of products that perform analysis on such data. Preventive measures to mitigate or eliminate future incidents are deployed during this phase, using industry best practices, data obtained from research and intelligence sources, and lessons learned from past incidents.

It is also imperative to prepare a list of contact information or notification methodologies to employ when an incident occurs, as well as notification and communication strategies within the team, with stakeholders, and with upper management and potentially other criminal justice and non-criminal justice agencies. This will help ensure that when incidents arise, the proper personnel and organizations are notified and kept informed of the circumstances regarding the incident.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Preparation phase can be given:

Malicious code execution

Preparation for incidents involving malicious code execution should initially involve user awareness of sources of malicious code. There are many potential sources of malicious code, such as web pages, emails, and removable media. The utilization and deployment of effective antivirus software, integrity-monitoring software, and intrusion detection and prevention software are effective measures to take to prepare for incidents involving malicious code execution.

Ransomware execution

Preparation phase activities for incidents involving ransomware execution are much the same as activities for malicious code execution, as ransomware is a specialized form of malware that encrypts potentially important or critical files, with the intention of coercing a victim to pay for a decryption key. Implementing a robust offline backup solution for these types of files is an important preparative action to take regarding the execution of ransomware. This will ensure that when ransomware attacks do happen, the mission impact is as minimal as possible and very little or no data is lost.

Denial of service attack

Denial of service attacks are given attention in the preparation phase. Defensive responses to denial of service attacks typically involve the use of a combination of attack detection and traffic classification and response tools, aiming to block traffic identified as abusive denial of service activity. Deploying solutions such as IDS/IPS devices and software, network hardware with rate-limiting capabilities (routers, switches, and firewalls), and upstream filtering devices at the system perimeter can mitigate for denial of service attacks.

Social Engineering

Preparation for social engineering attacks starts with user awareness training. Understanding and identifying attempts to obtain information in an unauthorized manner is crucial to thwarting these types of scenarios. Social engineering is the art of manipulating people to obtain information they may not be authorized to handle. Training and routinely testing users on potential social engineering scenarios and tactics, and providing training regarding appropriate responses to requests involving personal or otherwise sensitive information (for example, passwords or criminal justice information), is an effective way to ensure social engineering attacks never traverse past the preparation phase of the incident response life cycle.

Phishing

Like social engineering, preparation for phishing attacks is imperative. Phishing is a social engineering technique attackers employ to deceive users, in a fraudulent attempt to obtain sensitive information, or to gain unauthorized access to systems. Phishing is extremely widespread, and attackers disguising fraudulent scenarios in electronic communication such as email and instant messages are the most common. User awareness of these types of tactics is paramount to prepare for phishing attacks and schemes.

Detection and Analysis

The detection and analysis phase begins when a security incident has occurred. To understand when this phase begins, there must be a capability for an intelligent determination of circumstances constituting a security incident. Specialized knowledge and highly trained personnel are necessary for this step to be effective. Many organizations employ teams of personnel who are specifically trained to handle the intricacies of the incident response life cycle. The determination of a security incident can arise from one or several circumstances simultaneously – for example:

- Trained personnel manually reviewing collected event data for evidence of compromise
- Software applications analyzing events, trends, and patterns of behavior
- The observation of suspicious or anomalous activity on a computer system

The goals of this phase are:

- To detect whether a security incident occurred
- To determine the vector (i.e., method) of attack
- To determine the impact of the incident to the mission, systems, and personnel involved in the incident
- To obtain or create intelligence products regarding attack vectors and methodologies, especially when dealing with malicious code

Prioritization of incidents is also an important decision point in the incident response life cycle, as the circumstances regarding an incident can bring the situation to a critical level. There are three major impacts to consider when addressing priority of incidents:

- Functional Impact: the impact to business functionality
- Information Impact: the impact to confidentiality, integrity, and/or availability of criminal justice information
- Recoverability: the amount of time and resources that must be spent on recovering from an incident

Documentation regarding an incident should be thorough and applicable to the incident. This can be crucial in incidents that may lead to legal prosecution, as well as being invaluable to efficiently document, track, handle, manage, and resolve one or more incidents at the same time.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Detection and Analysis phase are given:

Malicious code execution

Detection of malicious code execution is often a primary job of host-based antivirus software. Having a capable and up-to-date antivirus solution installed on a system can detect known malicious code, as well as detect potentially malicious behaviors. The delivery of malicious code to a system can be detected by network traffic analysis and protection tools and hardware. Additionally, some malicious code may produce network traffic that is indicative of successful execution, exploitation, and/or compromise of a system. Solutions such as intrusion detection/prevention systems, Security Information and Event Management (SIEM) tools, and file integrity monitoring software can provide the necessary level of fidelity to make a determination of malicious code execution.

Knowing if or when a system is infected is not always immediately evident. Security controls may have been bypassed or even disabled by the malicious code. However, systems infected by malicious code or software (i.e. malware) can exhibit several indicators. These indicators include, but are not limited to:

Unexpected pop-up windows

Slow start up and/or slow performance

Suspicious hard drive activity including an unexpected lack of storage space

Missing files

Crashes and/or error messages

Unexplained network activity

Hijacked email

Analysis of malicious code can be performed in several ways. Static analysis of malicious code can be performed to determine the capabilities of the malicious code and generate actionable intelligence. Dynamic analysis of malicious code can be used to observe how the malicious code interacts with the system and what actions it performs and can often more rapidly determine the capabilities of malicious code. Both static and dynamic analysis can be performed manually, as well as in an automated fashion. Trained specialized personnel are crucial to the analysis of malicious code.

Ransomware execution

The detection of ransomware is identical to the detection of malicious code. Ransomware is specialized malicious code that encrypts potentially valuable files, generally with the intent to coerce a victim to pay a ransom for the possibility of the decryption of those files. Host-based antivirus solutions can also detect these threats, and network traffic analysis and protection tools and hardware can be used to prevent the successful execution of ransomware. SIEM tools and file integrity monitoring software can also detect the execution of ransomware.

Analysis of ransomware is identical to the analysis of malicious code, and the same intelligence can be determined in the same fashion as with the analysis of malicious code. The most obvious sign that ransomware has affected a system is the existence of encrypted files, the disappearance of certain types of files, and/or the presence of "ransom notes" on the system, which contain instructions for payment to obtain a decryption key, which may or may not be legitimate.

Denial of service attack

Denial of service (DoS) attacks are often detected at the perimeter of an organization but can also be detected within the organization as well. Often, from a user's perspective, the signs of a DoS attack appear to be network performance or administrative maintenance related issues such as slow or broken network connections or down websites. Additionally, an administrator may notice ping time outs, event logs overflowing or alerts from network monitoring systems as issues that may identify a DoS attack. Intrusion detection and prevention software and platforms can detect denial of service attacks, as well as some network monitoring hardware and appliances, such as web application filters, routers,

firewalls, and switches. Devices targeted by denial of service attacks can also detect the attacks in some instances, if they have the capabilities to determine explicit attack activity versus normal network traffic.

Analysis of denial of service attacks include the determination of the source traffic, the protocols used to generate the traffic, the service(s) targeted by the attack, and the potential impacts of the attack. Network monitoring devices can often provide these types of data, with the exception of potential impacts of denial of service attacks on systems.

Social Engineering

Detection of social engineering attacks is primarily based on the situational awareness of the individual targeted by social engineering. Given that social engineering is a broad topic that can involve the manipulation and exploitation of people in control of an information system, user awareness of social engineering attempts is crucial. If the target has security awareness training in detecting attempts to gain information or access in an unapproved manner, social engineering is easier to detect.

Analysis of social engineering attacks will generally rely on the recollection abilities of or documentation taken by the targets of the attack. Social engineering may not occur on an information system and may be completely carried out in-person. If the target can recollect or produce documentation regarding the social engineering attempt, the motivation and desired access can potentially be determined. For successful social engineering attempts, recollection and documentation of the attempt is crucial to determining the level of unauthorized access that was obtained.

Phishing

Detection of phishing attacks generally will first occur at an organization's email point of presence. Some organizations still run their own email servers, and many have migrated to cloud solutions. Having an on-premise email server or server farm or cluster will require additional functionality to detect phishing attempts. For example, the header content of the email will need to be read, as well as the content inside the body of the email, to check for potentially malicious content and potentially falsified data that may indicate a phishing email. Many cloud email providers have built this capability into their email solutions, but it is still possible for users to receive phishing emails, as attacker tactics and capabilities evolve daily. The most effective detection of phishing comes from heightened situational awareness of potential attacks. Validating the source of the email can uncover potential phishing attempts.

Analysis of phishing attacks involves examination of email headers, as well as contents of the body of the email. The body of the email may contain malicious content, attachments, or links to suspicious or malicious content. Manual or automated analysis activities can be

performed on the email content. Analysis of these elements should be performed by trained specialized personnel to generate intelligence and aid with the determination of indicators of compromise.

Containment, Eradication, and Recovery

Containment activities for computer security incidents involve decision-making and the application of strategies to help control attacks and damage, cease attack activities, or reduce the impact or damage caused by the incident. Often, this requires intelligence gathered by the detection and analysis phases of the incident – for example, identification of affected hosts, identification of attacking hosts or attackers, identification of malware and its capabilities, and identification and monitoring of attacker communication channels can be invaluable to the implementation of containment activities. In most cases, it is important to introduce containment solutions all at once, as attackers may escalate their attack activity if deployment of the strategy is delayed.

Eradication efforts for a computer security incident involve removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

Recovery efforts for incidents involve restoration of affected systems to normal operation. This may include actions like restoring systems from backups, rebuilding systems from an agency-approved baseline, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host-based security.

Compromised hosts are often attacked during these phases, as attackers try to regain their foothold on compromised systems or systems on the same network or others in the logical vicinity.

Malicious code execution

Containment activities for malicious code execution involve the logical or physical isolation of the host from the attacker's control and from any mission services or systems that would be impacted by the compromised host. This may include putting the host in a restricted VLAN, using firewalls to block traffic, disconnecting it from the network completely, shutting it down, or disabling functionality. Exercise caution as malicious code may have capabilities to take further actions on a host in case communications with a command and control server are severed. It is important to understand the capabilities of the malicious code before taking containment actions.

Eradication activities include the removal of malicious code from the system. This may be as simple as removing files, configuration rules, accounts, and other persistent items that the malicious code utilizes to function and maintain a presence on the system. This phase

also involves the discovery and removal of indicators of compromise on other systems, if applicable. It is imperative to remediate vulnerabilities that may have been exploited during eradication as well.

Recovery from malicious code execution generally is similar across many environments. Rebuilding the system from a clean baseline or restoring files from backup are typical activities that help restore the functionality of the system to continue the mission. Changing system passwords, installing patches, implementing tighter network access control, and ensuring appropriate levels of logging fidelity of the information system are integral parts of the recovery process.

Ransomware execution

Containment for ransomware execution should be as swift and immediate as possible, as ransomware can execute and spread to accessible media at a rapid pace. Considering files are being encrypted or have already been encrypted, immediate action should be taken to logically or physically isolate the system by disconnecting network connectivity. It is up to the system owner whether to take the risk in powering off the system, as valuable forensic artifacts may be destroyed in the process, but it will halt the execution of the ransomware and protect potentially valuable files. Please note that containment of active ransomware execution is one of the only circumstances where measures such as immediate shutdown are recommended.

Eradication of ransomware does not need to occur in most circumstances, as the entire goal of ransomware is to encrypt files and leave "recovery" instructions to extort victims. The vast majority of ransomware will delete itself once encryption of files is complete, but it is possible that some ransomware is persistent and can remain on the system. If this is the case, analysis should be performed on the ransomware to determine its capabilities, and eradication activities will proceed in an identical fashion to malicious code execution eradication activities.

Recovery from ransomware execution involves restoring encrypted files from backup and may involve the rebuilding of an entire system depending on the extent of the encryption from the ransomware. If a robust offline backup solution for hosts is not present or not utilized on a regular basis, the loss of potentially valuable data may be incredibly costly in several areas to repair, to include man-hours, revenue, and business products, data, and intelligence.

Denial of service attack

Containment of denial of service attacks involve the modification of access control where the attack is occurring. For example, if a web or application server is experiencing a denial of service attack, the system itself, as well as network monitoring devices, should be

examined to determine the source of the attack traffic. Once the source of the traffic is identified, modifications to access controls or rate-limiting features such as firewall access controls lists (ACLs) and web application filters can be employed to block the traffic. Care must be taken to determine if the observed traffic is actually intentional malicious denial of service traffic, versus heavy legitimate network traffic. Implementing access control mechanisms or rate-limiting features may negatively affect the mission of the system. It is also important to note that manual containment in this fashion may not be entirely effective, as attackers can circumvent the ACL by changing the attacking IP address, protocol, or other attribute of the connection.

Eradication is not necessarily applicable in denial of service scenarios, unless a vulnerability or misconfiguration is being exploited to cause the denial of service condition. If this is the case, take steps to remediate the vulnerability or misconfiguration.

Recovery actions depend on the available resources of the information system. For example, on-premise load balancers can be used to distribute the traffic, whether legitimate or malicious, to other less-burdened systems. Many cloud providers and content delivery networks also have denial of service mitigation capabilities. It may also be prudent to increase the resources (memory, processing capacity) of internet-facing systems so that they can handle larger amounts of traffic simultaneously.

Social Engineering

Containment regarding social engineering attacks is dependent upon the information or access that was provided to the attacker. For example, if an attacker gained access to an account on a system following a social engineering attempt, the account should be administratively disabled and all sources of event data regarding that account should be immediately collected. If sensitive data was divulged to the attacker, the impact of the exposure of that data should be examined and mitigating activity should be initiated to determine or reduce the damage of the spread of the information.

Eradication regarding social engineering attacks also depends on the information or access provided to the attacker. Removing or limiting the provided access is a pertinent eradication action. If the information provided is a credential to a system, disable and remove the credential from the system. Eradication may also involve the physical detainment or removal of personnel from a site.

Recovery actions for social engineering attacks are dependent on the information or access provided to the attacker. Additionally, security awareness training is an appropriate recovery action to ensure staff understands the threats of social engineering.

Phishing

Containment of phishing activity is tied very closely to the identification and analysis of the phishing activity. Understanding the tactics of the phishing attacker is paramount to deploying containment activities. Activities include, but are not limited to, administratively blocking sender email addresses and IPs, blocking potential malicious content in email via a web proxy, communicating with potential recipients, and implementation of email content or hyperlink blacklisting if possible. Phishing attacks can also include attempts to have users execute malicious code on systems, where containment activities regarding malicious code will be applicable.

Eradication of phishing attacks include the administrative removal of the emails from email systems, as well as eradication actions for malicious code if applicable.

Recovery from phishing attacks can include:

- Implementation and enforcement of the Domain Keys Identified Mail (DKIM) email authentication method, which can mitigate the possibility that attackers can send spoofed email
- Implementation and enforcement of Sender Policy Framework (SPF) to control and stop sender forgeries
- Implementation and enforcement of Domain-based Message Authentication, Reporting, and Conformance (DMARC), which enables message senders to indicate that their messages are protected with SPF and/or DKIM

Additionally, if malicious code is present in the phishing attack, recovery actions regarding malicious code may be applicable.

Post-Incident Activity

Post-incident activities occur after the detection, analysis, containment, eradication, and recovery from a computer security incident. Arguably one of the most important phases of incident response, post-incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident, including the incident response team. Some of the important items to consider:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?

- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar actions in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Smaller incidents, and those that are similar to others that have been well documented, do not necessarily need much focus in this phase of incident response. Larger and less-understood security incidents should be the focus of a comprehensive post-mortem evaluation that outlines many of the items listed above and should include personnel that can have a direct impact on or are directly affected or responsible for the involved systems.

Post-incident activities such as these also help to serve as training opportunities for all parties involved in the incident, from victims, to system administration personnel, to incident responders.

Malicious code execution

Post-incident activities for malicious code execution generally will follow similar patterns. A timeline of activity should have been prepared using digital forensic data collected during the detection and analysis phases of the incident. This timeline should include all affected systems and times of all activities and actions taken during the incident. Steps that victims and system administrators may have taken during the course of the incident, as well as in close proximity to the time range of the incident, are valuable items to document and discuss. Any deviation from organizational policy should be noted and taken as training items or assigned consequences in accordance with organizational policies. It may also be pertinent to ensure that appropriate information and intelligence sharing was performed during and after the incident occurred. Corrective actions that may have prevented the execution of malicious code, such as antivirus solutions, restrictions on where executables can run, tightened permissions, and script blockers for browsers, should be considered as a mitigation for the risks posed by malicious code threats. Web proxy blocks from information discovered during analysis can be utilized to ensure that malicious hosts are not contacted.

Ransomware execution

Post-incident activities for ransomware execution include all the activities involved with malicious code execution, with the addition of ensuring the functionality of a robust offline backup solution. An offline backup solution ensures that backup data is kept inaccessible to ransomware threats and is available if ransomware is successfully executed. A functional and frequent (such as daily incremental and weekly full) backup process helps ensure that business continuity is maintained in the event of issues and incidents.

Denial of service attack

Denial of service post-incident activities should include a timeline of traffic activities, as well as organizational responses to the attack traffic as well as the timeline of any business impacts and the damage associated with the impacts. Any attack precursors should be investigated and noted, and intelligence implemented to notify personnel and potentially take action as soon as attack traffic is observed. Impacts on affected systems should be noted, and a consensus should be reached on whether the systems should be upgraded or supplemented with load-balancing capabilities.

Social Engineering

Post-incident activities for social engineering incidents should include a timeline that includes all applicable activities, such as points of contact, narratives from the parties involved, CCTV footage (if applicable), system and network log files, and physical access control logging data. If unauthorized access was obtained, the impact of the access should be assessed and mitigating factors should be identified for inclusion to reduce the risk of future incidents (such as multifactor authentication, physical locks, greater CCTV coverage, improved physical access control, etc.). Security awareness training should be imperative if policy was breached, and information or access was given to unauthorized parties.

Phishing

Phishing post-incident activities should also include a timeline of actions taken since the phishing email was received, to include descriptions of the type of phishing campaign observed (malicious code, financial exploitation, credential harvesting, etc.), malicious attachments contained (if any), malicious or suspicious links in the body of emails, as well as narratives from recipients of the email and any potential victims, either self-reported or discovered through email, network, or host-based monitoring. If malicious code was included in the campaign, typical post-incident activities involving malicious code should be considered as well. Training opportunities can often arise from phishing attacks, whether successful or not, that can be valuable in giving employees better situational awareness regarding phishing.

The CJIS Security Policy requires each agency with access to CJI to establish operational incident handling procedures (i.e. a local policy). Gleaning from the requirements in Section 5.3 Incident Response, the local policy may include the following elements:

- Overall incident handling procedures. This section describes and identifies the processes used locally how the agency successfully prepares for, manages, and recovers from an incident. It includes sections on:
    - Preparation
    - Detection and Analysis
    - Containment

    - Recovery
    - User response activities
- How the agency performs incident reporting. This section describes the process of notifying internal and external partners when an incident has occurred and how the incident is documented. It includes sections on:
    - Internal and external points of contact
    - Required tracking and reporting documents
    - Escalation procedures
- Incident management procedures. This section describes the agency's approach to a consistent and repeatable approach to managing incidents. It includes sections on:
    - Roles and responsibilities
    - Incident-related information collection
    - Updating policies with lessons learned
    - Collection of evidence
    - Incident response training
    - Document and artifact retention

G.8 Secure Coding

Secure Coding

This appendix documents a source of information on best practices and standards for secure coding. With the increased use of software products and the rapid pace of modern software development, it is essential to discover and resolve insecure software risks. The mitigations and guidelines to reduce these common risks can be found in secure coding best practices.

Understanding how software applications work can be a daunting thing; however, it could be key to know if data security is in jeopardy. Awareness of secure coding practices allows an agency to review potential vendors and their products prior to purchase and implementation. It also empowers the agency with the knowledge of the questions to ask a vendor of how the software was developed and whether the vendor uses secure coding practices or standards.

Additionally, the information in this appendix can provide a path forward for agencies with the internal capability to produce "in-house" software applications. By implementing security during the code writing process, security is "baked in" and there is more trust the software will aid in protecting the information it processes.

Open Web Application Security Project (OWASP) Foundation

The OWASP Foundation is a not-for-profit charitable organization focused on improving the security of software. OWASP operates as a community of like-minded professionals to provide unbiased and practical information about application security (AppSec) through software tools and documentation. These materials are available under a free and open software license, which can be located at the link below.

https://www.owasp.org/index.php/Main_Page

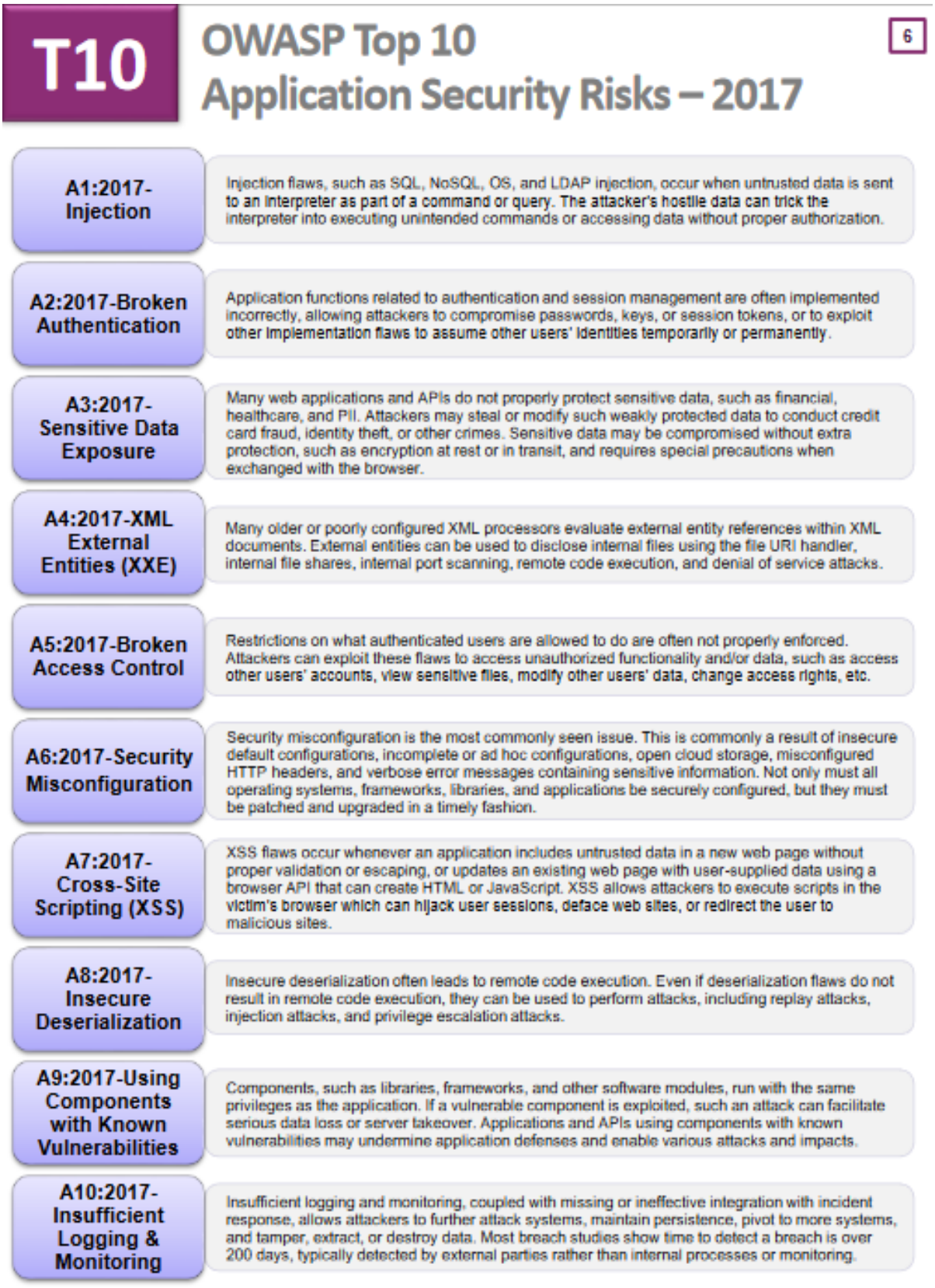
Software is becoming increasingly complex and connected, and the difficulty of achieving application security increases exponentially. The rapid pace of modern software development processes makes the most common risks essential to discover and resolve quickly and accurately.

The OWASP Foundation publishes the Top 10 Application Security Risks, which focus on the most serious web application security risks. The OWASP Top 10 is based primarily on 40 plus data submissions from firms that specialize in application security and an industry survey that was completed by over 500 individuals. This data spans vulnerabilities gathered from hundreds of organizations and over 100,000 real world applications and application program interfaces (API). The Top 10 items are selected and prioritized according to this data, in combination with consensus estimates of exploitability, detectability, and impact.

A primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risks problem areas, and provides guidance on a path forward.

The OWASP Top 10 focuses on identifying the most serious web application security risks for a broad array of organizations. For each of these risks, generic information about likelihood and technical impact using the following simple ratings scheme, which is based on the OWASP Risk Rating Methodology.

Figure G.8-A


T10
OWASP Top 10
Application Security Risks – 2017
6
A1:2017-Injection
Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2:2017-Broken Authentication
Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
A3:2017-Sensitive Data Exposure
Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
A4:2017-XML External Entities (XXE)
Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
A5:2017-Broken Access Control
Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
A6:2017-Security Misconfiguration
Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.
A7:2017-Cross-Site Scripting (XSS)
XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A8:2017-Insecure Deserialization
Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
A9:2017-Using Components with Known Vulnerabilities
Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
A10:2017-Insufficient Logging & Monitoring
Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Each organization is unique, and so are the threat actors for that organization, their goals, and the impact of any breach. It is critical to understand the risk to your organization based on applicable threat agents and business impacts.

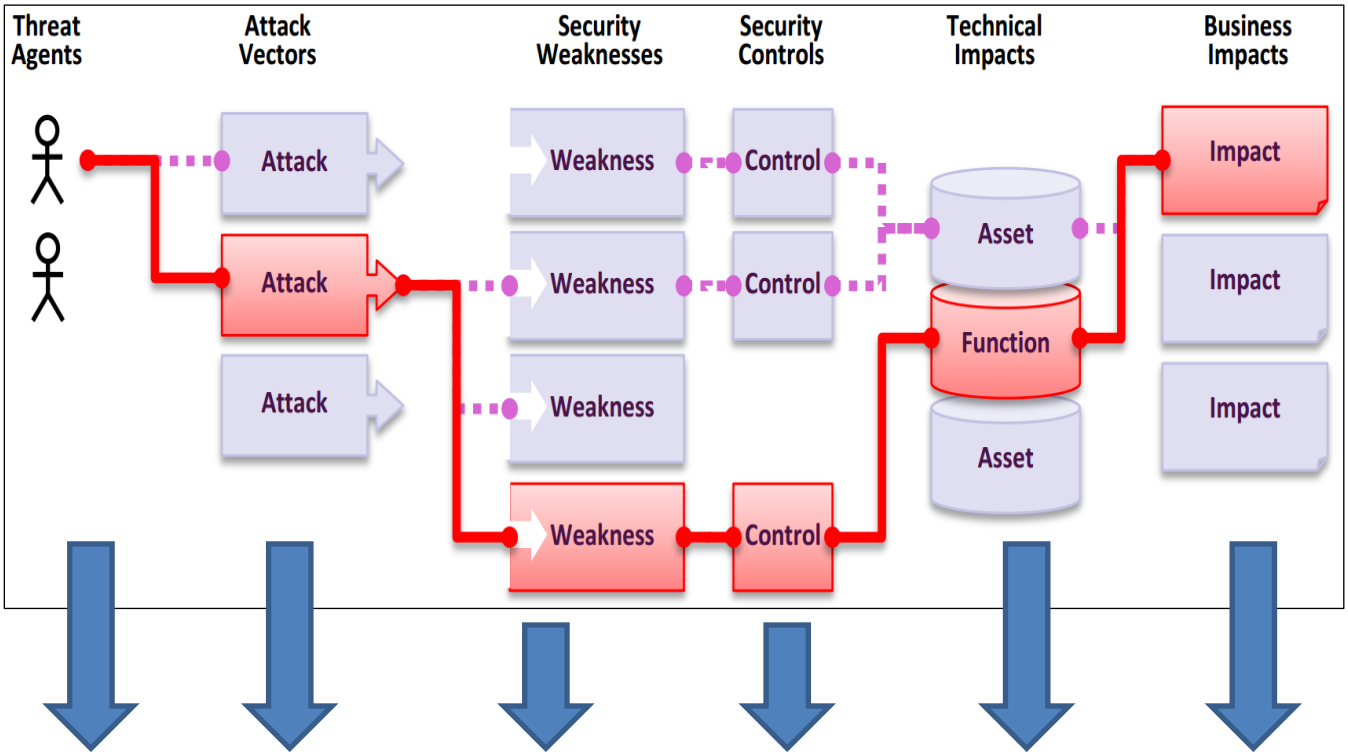
Application Security Risks

The figures immediately below illustrate the path of a sample threat beginning with the threat agent and ending with the target or affected business resource. Various paths are available but the agent would normally select the path of least resistance which would be the most vulnerable and with the fewest number of effective security controls.

The sample risk matrix can be used to assign in the various aspects of potential vulnerability. Each column corresponds to a phase in the attack process. In the matrix, a lower value represents less risk and is more desirable.

Concerning secure coding practices, when security is built-in during code development, vulnerabilities can be identified and controls included reducing the overall risk to information processed by the code.

Figure G.8-B Sample Threat Path



Threat Agents	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	SEVERE: 3	App / Business Specific
	AVERAGE: 2	COMMON: 2	AVERAGE: 2	MODERATE: 2	
	DIFFICULT: 1	UNCOMMON: 1	DIFFICULT: 1	MINOR: 1	

Figure G.8-C General Risk Matrix

To understand these risks for a particular application or organization, you must consider your own specific threat agents and business impacts. Even severe software weaknesses may not present a serious risk if there are no threat agents in a position to perform the necessary attack or the business impact is negligible for the assets involved. The following table presents a summary of the 2017 Top 10 Application Security Risks, and the risk factors that have been assigned to each risk.

Figure G.8-D Top 10 Risk Factor Summary

RISK	Threat Agents	Attack Vectors	Security Weakness		Impacts		Score
		Exploitability	Prevalence	Detectability	Technical	Business	
A1:2017-Injection	App Specific	EASY: 3	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	8.0
A2:2017-Authentication	App Specific	EASY: 3	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A3:2017-Sens. Data Exposure	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE: 2	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	MODERATE: 2	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2	WIDESPREAD: 3	DIFFICULT: 1	MODERATE: 2	App Specific	4.0

Whether you are new to web application security or already very familiar with these risks, the task of producing a secure web application or fixing an existing one can be difficult. If you have to manage a large application portfolio, this task can be daunting.

To help organizations, developers, testers and managers reduce their application security risks in a cost-effective manner; OWASP has produced numerous free and open resources that you can use to address application security in your organization. The following are some of the many resources OWASP has produced to help organizations produce secure web applications and APIs.

Get Started:

- Document all applications and associated data assets.
- Larger organizations should consider implementing a Configuration Management Database (CMDB).
- Establish an application security program to conduct analysis to define key improvement areas and an execution plan.

Risk Based Portfolio Approach:

- Identify the protection needs of your application portfolio from a business perspective.
- Establish a common risk-rating model with a consistent set of likelihood and impact factors reflective of your organization's tolerance for risk.
- Measure and prioritize all applications and APIs and add results to CMDB.

Enable with a Strong Foundation:

- Establish a set of policies and standards that provide an application security baseline for all development teams to adhere too.
- Define a common set of reusable security controls that complement these policies and standards and provide design and development guidance on their use.

Integrate Security into Existing Processes:

- Define and integrate secure implementation and verification activities into existing development and operational processes.
    - Activities include threat modeling, secure design and design review, secure coding and code review, penetration testing, and remediation.

Application Security Requirements - to produce a secure web application, you must define what secure means for that application.

- Application Security Verification Standard (ASVS):
  https://www.owasp.org/index.php/ASVS

- OWASP Secure Software Contract Annex:
  https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

Application Security Architecture - retrofitting security into your applications and APIs, it is far more cost effective to design the security in from the start.

- OWASP Prevention Cheat Sheets:

https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series

Standard Security Controls - building strong and usable security controls is difficult. Using a set of standard security controls radically simplifies the development of secure applications and APIs.

- OWASP Proactive Controls:
  https://www.owasp.org/index.php/OWASP_Proactive_Controls

Secure Development Lifecycle - to improve the process your organization follows when building applications and APIs, organizations formulate and implement a strategy for software security that is tailored to the specific risks facing their organization.

- OWASP Software Assurance Maturity Model (SAMM):
  https://www.owasp.org/index.php/OWASP_SAMM_Project

- OWASP Application Security Guide for CISOs:
  https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs

Application Security Education – hands-on learning about vulnerabilities to help educate developers on web application security.

- OWASP Education Project:

  https://www.owasp.org/index.php/Category:OWASP_Education_Project

- OWASP WebGoat:
  https://www.owasp.org/index.php/WebGoat

- OWASP Broken Web Application Project:
  https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project

Understand the Threat Model – be sure to understand the priorities when it comes to threat model.

- OWASP Testing Guide:
  https://www.owasp.org/index.php/OWASP_Testing_Project

- Application Security Verification Standard (ASVS):

  https://www.owasp.org/index.php/ASVS

Testing Strategies – choose the simplest, fastest, most accurate technique to verify each requirement.

- OWASP Security Knowledge Framework:
  https://www.owasp.org/index.php/OWASP_Security_Knowledge_Framework

- Application Security Verification Standard (ASVS): https://www.owasp.org/index.php/ASVS

APPENDIX H SECURITY ADDENDUM

The following pages contain:

The legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4);

An example of a contract addendum (H-5);

The Security Addendum itself (H6-H7);

The Security Addendum Certification page (H8).

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

Legal Authority for and Purpose and Genesis of the Security Addendum

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

> 1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.
>
> We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security

addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:

1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.

2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and

3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power

and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

EXAMPLE OF A CONTRACT ADDENDUM

AMENDMENT NO. ___ TO THE CONTRACT BETWEEN
[PARTY NO. 1] AND [PARTY NO. 2], ENTERED INTO [DATE]

[Name of Law Enforcement Agency] and [Party No. 2], upon notification and pursuant to Paragraph/Section No. ___ [the amendment clause of the original contract] of that certain contract entered into by these parties on [date][and entitled "___"], hereby amend and revise the contract to include the following:

1. Access to and use of criminal history record information and other sensitive information maintained in [state and] FBI-managed criminal justice information systems by [private party] are subject to the following restrictions:

a.

b.

c.

and

d. The Security Addendum appended hereto, which is incorporated by reference and made a part thereof as if fully appearing herein.

This amendment is effective the ____ day of _____, 20__.

On behalf of [Party No. 1]: _____

[Name]

_____

[Title]

_____

Date

On behalf of [Party No. 2]: _____

[Name]

_____

[Title]

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION

CRIMINAL JUSTICE INFORMATION SERVICES

SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative

APPENDIX I REFERENCES

White House Memo entitled "Designation and Sharing of Controlled Unclassified Information (CUI)", May 9, 2008

[CJIS RA] *CJIS Security Policy Risk Assessment Report*; August 2008; For Official Use Only; Prepared by: Noblis; Prepared for: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26306

[CNSS Instruction No. 4009] *National Information Assurance (IA) Glossary*; Committee on National Security Systems (CNSS) Instruction No. 4009; 26 April 2010

[FBI SA 8/2006] *Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum*; 8/2006; Assistant Director, Criminal Justice Information Services, FBI, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306

[FISMA] *Federal Information Security Management Act of* 2002; House of Representatives Bill 2458, Title III–Information Security

[FIPS 199] *Standards for Security Categorization of Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 199; February 2004

[FIPS 200] *Minimum Security Requirements for Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 200; March 2006

[FIPS 201] *Personal Identity Verification for Federal Employees and Contractors*; Federal Information Processing Standards Publication, FIPS PUB 201-1

[NIST SP 800–14] *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST Special Publication 800–14

[NIST SP 800–25] *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*; NIST Special Publication 800–25

[NIST SP 800–30] *Risk Management Guide for Information Technology Systems*; NIST Special Publication 800–36

[NIST SP 800–32] *Introduction to Public Key Technology and the Federal PKI Infrastructure*; NIST Special Publication 800–32

[NIST SP 800–34] *Contingency Planning Guide for Information Technology Systems*; NIST Special Publication 800–34

[NIST SP 800–35] *Guide to Information Technology Security Services*; NIST Special Publication 800–35

[NIST SP 800–36] *Guide to Selecting Information Technology Security Products*; NIST Special Publication 800–36

[NIST SP 800–39] *Managing Risk from Information Systems, An Organizational Perspective*; NIST Special Publication 800–39

[NIST SP 800–40] *Procedures for Handling Security Patches*; NIST Special Publication 800–40

[NIST SP 800–44] *Guidelines on Securing Public Web Servers*; NIST Special Publication 800–44

[NIST SP 800–45] *Guidelines on Electronic Mail Security*; NIST Special Publication 800–45, Version 2

[NIST SP 800–46] *Security for Telecommuting and Broadband Communications*; NIST Special Publication 800–46

[NIST SP 800–48] *Wireless Network Security*: 802.11, *Bluetooth, and Handheld Devices*; NIST Special Publication 800–48

[NIST SP 800–52] *Guidelines on the Selection and Use of Transport Layer Security*; NIST Special Publication 800–52

[NIST SP 800–53] *Recommended Security Controls for Federal Information Systems*; NIST Special Publication 800–53, Revision 2

[NIST SP 800–53A] *Guide for Assessing the Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*; NIST Special Publication 800–53A

[NIST SP 800–58] *Security Considerations for Voice over IP Systems*; NIST Special Publication 800–58

[NIST SP 800–60] *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST Special Publication 800–60, Revision 1, DRAFT

[NIST SP 800–63–1] *Electronic Authentication Guideline*; NIST Special Publication 800–63–1; DRAFT

[NIST SP 800–64] NIST Special Publication 800–64

[NIST SP 800–66] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act* (HIPAA); NIST Special Publication 800–66

[NIST SP 800–68] *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*; NIST Special Publication 800–68

[NIST SP 800–70] *Security Configuration Checklists Program for IT Products*; NIST Special Publication 800–70

[NIST SP 800–72] *Guidelines on PDA Forensics*; NIST Special Publication 800–72

[NIST SP 800–73] *Integrated Circuit Card for Personal Identification Verification*; NIST Special Publication 800–73; Revision 1

[NIST SP 800–76] *Biometric Data Specification for Personal Identity Verification*; NIST Special Publication 800–76

[NIST SP 800–77] *Guide to IPSec VPNs*; NIST Special Publication 800–77

[NIST SP 800–78] *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*; NIST Special Publication 800–78

[NIST SP 800–81] *Secure Domain Name System* (DNS) *Deployment Guide*; NIST Special Publication 800–81

[NIST SP 800–84] *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*; NIST Special Publication 800–84

[NIST SP 800–86] *Guide to Integrating Forensic Techniques into Incident Response*; NIST Special Publication 800–86

[NIST SP 800–87] *Codes for the Identification of Federal and Federally Assisted Agencies*; NIST Special Publication 800–87

[NIST SP 800–96] *PIV Card / Reader Interoperability Guidelines*; NIST Special Publication 800–96

[NIST SP 800–97] *Guide to* IEEE 802.11i: *Robust Security Networks*; NIST Special Publication 800–97

[NIST SP 800–121] *Guide to Bluetooth Security*, NIST Special Publication 800-121

[NIST SP 800–124] *Guidelines on Cell Phone and PDA Security*, NIST Special Publication 800-124

[NIST SP 800-125] *Guide to Security for Full Virtualization Technologies*; NIST Special Publication 800-125

[NIST SP 800–144] *Guidelines on Security and Privacy in Public Cloud Computing*; NIST Special Publication 800-144

[NIST SP 800–145] *The NIST Definition of Cloud Computing*; NIST Special Publication 800-145

[NIST SP 800–146] *Cloud Computing Synopsis and Recommendations*; NIST Special Publication 800-146

[OMB A–130] *Management of Federal Information Resources*; Circular No. A–130; Revised; February 8, 1996

[OMB M–04–04] *E-Authentication Guidance for Federal Agencies*; OMB Memo 04–04; December 16, 2003

[OMB M–06–15] *Safeguarding Personally Identifiable Information*; OMB Memo 06–15; May 22, 2006

[OMB M–06–16] *Protection of Sensitive Agency Information*; OMB Memo 06–16; June 23, 2006

[OMB M–06–19] *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*; OMB Memo 06–19; July 12, 2006

[OMB M–07–16] *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; OMB Meme 07–16; May 22, 2007

[Surviving Security] *Surviving Security: How to Integrate People, Process, and Technology*; Second Edition; 2004

[USC Title 5, Section 552] *Public information; agency rules, opinions, orders, records, and proceedings*; United States Code, Title 5 - Government Agency and Employees, Part I - The Agencies Generally, Chapter 5 - Administrative Procedure, Subchapter II - Administrative Procedure, Section 552. Public information; agency rules, opinions, orders, records, and proceedings

[USC Title 44, Section 3506] *Federal Information Policy*; 01/02/2006; United States Code, Title 44 - Public Printing and Documents; Chapter 35 - Coordination of Federal Information Policy; Subchapter I - Federal Information Policy, Section 3506

APPENDIX J NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Noncriminal Justice Agencies (NCJA) with access to Criminal Justice Information (CJI) as authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes, via their State Identification Bureau (SIB) and/or Channeling agency. Examples of the target audience for the Appendix J supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc.

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to CJI maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those NCJAs new to the CSP and Advisory Policy Board (APB) auditing process (all NCJAs will be periodically audited by the CJIS Systems Agency (CSA)/SIB and may be included in a sampling of triennial audits conducted by the FBI*)* it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every NCJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific "shall" statement please go to the referenced section within the main body of the CSP.

General CJI Guidance

The following information provides NCJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. 3.2.9 – Local Agency Security Officer (LASO)

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local NCJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and

procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.6 – Agency User Agreements

When an NCJA (private or public) is permitted to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions as authorized pursuant to federal law or state statute approved by the U.S. Attorney General, the information received from the background check, such as criminal history record information (CHRI) or personally identifiable information (PII), must be protected as CJI. In order to receive access to CJI the NCJA must enter into a signed written agreement, i.e., an agency user agreement, with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the CJI access. An example of a NCJA (private) is a local bank. An example of a NCJA (public) is a county school board.

Note 1: The CSA, SIB, or authorized agency providing the CJI access term should be part of the agency user agreement.

Note 2: Any NCJA that directly accesses FBI CJIS must allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2.1.1 – All Personnel (Security Awareness Training)

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

Note: The CSO/SIB may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help NCJAs with:

(i) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,

(ii) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative

to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient. The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to electronic and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

"Electronic media" is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store electronic and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn't possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a criminal justice conveyance, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data "at rest") of CJI.

i. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.

Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record

information for the purposes of licensing or employment need to follow the guidance in Section 5.12 (referenced below).

j. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have unescorted access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring unescorted access to unencrypted CJI.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Agencies located within states that have not passed legislation authorizing or requiring civil fingerprint-based background checks are exempted from this requirement until such time as appropriate legislation has been written into law.

The following scenarios are intended to help the reader identify areas within the CSP that NCJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above General CJI Guidance section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.

Hard Copy CJI Storage and Accessibility

When an NCJA receives CJI via a paper copy from a CJA and stores the paper within a locked file cabinet, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

Electronic CJI Storage and Accessibility – Controlled Area

When an NCJA creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control – Encryption

CSP Section 5.5.2.4 item 3 – Encryption describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this situation. Encrypted information can only be read by personnel possessing the

appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

Electronic CJI Storage and Accessibility – Physically Secure Location

When an NCJA receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy sections:

a. 5.5 – Access Control

   CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. 5.6 – Identification and Authentication

   CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. 5.7 – Configuration Management

   CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

   CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

   CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. 5.10 – System and Communications Protection and Information Integrity

   CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency's environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

Use Case Scenarios

1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that has indirect access to CJI and is located in a secure data center within the board of education offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

Keeping in mind the scenario as described, an authorized user needs access to an employee's electronic record. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the record, the user is prompted to enter their unique username and password. Because the record resides on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required to access the record.

NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.

2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) encryption algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access an employee's record, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder.

NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.

APPENDIX K CRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Criminal Justice Agencies (CJA) that have historically not been subject to audit under the CJIS Security Policy guidelines. The target audience typically gains access to CJI via fax, hardcopy distribution or voice calls; does not have the capability to query state or national databases for criminal justice information; and may have been assigned an originating agency identifier (ORI) but is dependent on other agencies to run queries on their behalf. This guidance is not intended for criminal justice agencies covered under an active information exchange agreement with another agency for direct or indirect connectivity to the state CJIS Systems Agency (CSA) – in other words those agencies traditionally identified as "terminal agencies".

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to criminal justice information (CJI) maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those CJAs new to the CSP it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every CJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific "shall" statement please go to the referenced section within the main body of the CSP.

General CJI Guidance

The following information provides CJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. 3.2.9 – Local Agency Security Officer (LASO)

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local CJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.3 – Criminal Justice Agency User Agreements

Any CJA receiving access to CJI must enter into a signed agreement with the CSA providing the access. The agreement specifies the services and systems the agency will access. It must also specify all pertinent governance policies to which the agency must adhere.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2 – Security Awareness Training

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

CSP Section 5.2.1.2 describes the topics required to be discussed for personnel that have both physical and logical access to CJI. These topics are covered in addition to the ones addressed in basic security awareness training.

CSP Section 5.2.1.3 describes topics to be covered for those personnel assigned information technology roles. Topics covered in this section are in addition to the topics addressed in Sections 5.2.1.1 and 5.2.1.2.

Note: The CSO may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help CJAs with:

(iii) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,

(iv) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient.

The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to digital and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

"Digital media" is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store digital and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn't possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy digital media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a police vehicle, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data "at rest") of CJI.

i. 5.10 – System and Communications Protection and Information Integrity

CSP Section 5.10 explains the technical safeguards ranging from boundary and transmission protection to security an agency's virtualized environment.

CSP Section 5.10.1.2 details the requirements for the encryption of CJI whether in transit or at rest. FIPS 140-2 certification is required when CJI is in transit outside a physically secure location. When at rest outside a physically secure location, encryption methods can use Advanced Encryption Standard (AES) at 256 bit strength or a FIPS 140-2 certified method.

CSP Section 5.10.3 explains the use of virtualization and partitioning when processing CJI in a virtual environment. A virtualized environment can be configured such that those parts of the system which process CJI are either physically or virtually separated from those that do not.

CSP Section 5.10.4 explains system and information integrity policy and procedures. This includes areas such as patch management, malicious code protection, and spam and spyware protection.

j. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.

Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one

representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

k. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have unescorted access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring unescorted access to unencrypted CJI.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

l. 5.13 – Mobile Devices

When access to CJI using mobile devices such as laptops, smartphones, and tablets is authorized, CSP Section 5.13 explains the controls required to manage those devices to ensure the information remains protected.

The following scenarios are intended to help the reader identify areas within the CSP that CJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above "General CJI Guidance" section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.

Hard Copy CJI Storage and Accessibility

When CJI is received in hard copy and the agency stores the paper within a locked file cabinet, the CJA should, in addition to the "General CJI Guidance", focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

Electronic CJI Storage and Accessibility – Controlled Area

When an agency creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the agency should, in addition to the "General CJI Guidance", focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control Mechanisms – Encryption

CSP Section 5.5.2.4 item 3, Encryption – This describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this

situation. Encrypted information can only be read by personnel possessing the appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

Electronic CJI Storage and Accessibility – Physically Secure Location

When an agency receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the agency should, in addition to the "General CJI Guidance", focus on compliance with policy sections:

a. 5.5 – Access Control

   CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. 5.6 – Identification and Authentication

   CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. 5.7 – Configuration Management

   CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

   CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

   CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. 5.10 – System and Communications Protection and Information Integrity

   CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency's environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

Use Case Scenarios

1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

   A county court scans hard copy case documents containing CJI into an electronic format. The documents are placed on a network server which is located in a secure data center within the court offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

   Keeping in mind the scenario as described, an authorized user needs access to case documents. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the documents, the user is prompted to enter their unique username and password. Because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

   NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.

2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

   A county court scans hard copy case documents containing CJI in an electronic format. The documents are placed on a network server which is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

   To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access to the case documents, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder. Additionally, because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

   NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.

Death Scene Checklist.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

MADISON COUNTY SHERIFFS OFFICE
DEATH SCENE CHECKLIST

Updated: 01/05/2021
MCSO-DOA

CASE INFORMATION

Case #:	**Date:**	**Offense #:**
Dispatch Time:	**Arrival Time:**	**Forensics Arrival Time:**
Location:		
Investigating Deputy:	**Supervisor Notified:**	

NATURAL DEATHS

Deputy Completing DSCL:

STOP & NOTIFY INVESTIGATIONS

HOMICIDE, SUICIDE, SUSPICIOUS, CHILD, ETC DEATHS

Crime Scene Secured: ☐
Scene Log Started: ☐ Log Officer:
Forensic Point of Contact Notified: ☐
Forensic Personnel On Scene:
Forensic Supervisor:
Officer/Detective Completing DSCL:

DECEDENT INFORMATION

Name:		**Alias (if any):**		
Address:		**Phone #s:**		
DOB:	**SSN:**	**Race:**	**Sex:**	**Marital Status:**

DECEDENT FOUND BY INFORMATION

Relationship to Decedent:	**Date Found:**	**Time Found:**	**Time CPD Notified:**

Name:		**Alias (if any):**		
Address:		**Phone #s:**		
DOB:	**SSN:**	**Race:**	**Sex:**	**Marital Status:**

DECEDENT LAST SEEN ALIVE BY INFORMATION

Relationship to Decedent:	**Date Seen:**	**Time Seen:**	**Location:**

Name:		**Alias (if any):**		
Address:		**Phone #s:**		
DOB:	**SSN:**	**Race:**	**Sex:**	**Marital Status:**

NEXT OF KIN NOTIFICATION INFORMATION

Relationship to Decedent:	**Date Notified:**	**Time Notified:**	**Notified By:**
Next of Kin Identification of Decedent: Yes: ☐ **No:** ☐ **Other Identification Made:**			

Name:		**Alias (if any):**		
Address:		**Phone #s:**		
DOB:	**SSN:**	**Race:**	**Sex:**	**Marital Status:**

SCENE CONDTIONS

SCENE TYPE: ☐ HOUSE ☐ APARTMENT ☐ FIELD/WOODS ☐ OFFICE/COMMERCIAL
☐ STREET/ALLEY ☐ VEHICLE ☐ OTHER (DESCRIBE): _____

1ST DEPUTY ENTRY METHOD: ☐ DOOR ☐ WINDOW ☐ OTHER (DESCRIBE): _____
☐ UNLOCKED ☐ KEY ☐ FIRST RESPONDER FORCED ENTRY
NOTES: _____

CONDITION OF DOORS

DOOR LOCATION	OPEN/CLOSED	LOCKED/UNLOCKED	DAMAGED

Forensic Unit Personnel: Photograph All Doors, Locks, & Damage If Forced Entry on All Non-Natural Death

CONDITION OF WINDOWS:

WINDOW LOCATION	OPEN/CLOSED	LOCKED/UNLOCKED	DAMAGED

Forensic Unit Personnel: Photograph All Windows, Locks, & Damage If Forced Entry on All Non-Natural Deaths

HEATING & AIR CONDITIONING:

HEAT & AC SETTINGS: _____ DISPLAY TEMP: _____ ROOM TEMP: _____
HEAT & AC SOURCES NEAR DECEDENT: _____
All Officers: Photograph Heat & AC Control Unit If Possible on all Death Scenes

CONDITION OF SURROUNDINGS:

☐ ORDERLY ☐ LIVED-IN ☐ DISARRAY ☐ HOARDING
DESCRIBE: _____
☐ RANSACKED (POSSIBLE ROBBERY/BURGLARY)
☐ FIRE (ANY FIRE SCENE WHERE A DECEDENT IS LOCATED)
IF RANSACKED OR FIRE SECURE SCENE & NOTIFY FORENSIC POINT OF CONTACT
DESCRIBE: _____
☐ DATED MATERIAL: ☐ NEWSPAPERS & DATES: _____
☐ MAIL INSIDE & DATES: _____
☐ MAIL OUTSIDE & DATES: _____
☐ FOOD PREP: _____
☐ FOOD ROTTING: _____
ODORS UPON ENTRY: ☐ DECOMPOSITION ☐ PET ODORS ☐ OTHER: _____
☐ CLEANING PRODUCTS (DESCRIBE): _____
☐ FIRE OR OTHER BURNING (DESCRIBE): _____

CONDITION OF LIGHTING & ELECTRONICS:

_____ ON: ☐ _____ ON: ☐ _____ ON: ☐
_____ ON: ☐ _____ ON: ☐ _____ ON: ☐

DECEDENT LOCATION & CONDITION

DECEDENT FOUND IN:
☐ LIVING ROOM ☐ DINING ROOM ☐ BEDROOM ☐ KITCHEN
☐ CLOSET ☐ OFFICE/STUDY ☐ BASEMENT ☐ GARAGE
☐ SHED/EXTERIOR AREA (DESCRIBE): _____
☐ BATHROOM (OTHER THAN SHOWER/TUB)
☐ BATHROOM SHOWER/TUB
☐ POOL/OTHER BODY OF WATER

DECEDENT POSITION:
☐ ON BACK ☐ FACE DOWN ☐ ON SIDE (Left or Right) ☐ SEATED
☐ OTHER (DESCRIBE): _____

DECEDENT CLOTHING:
☐ FULLY CLOTHED ☐ NUDE
☐ PARTIALLY CLOTHED (CLOTHING MISSING): _____
☐ TORN/DAMAGED CLOTHING: _____

DECEDENT BY TOUCH:
☐ WARM ☐ COOL ☐ ROOM TEMPERATURE

POSTMORTEM CHANGES:

BODY COLOR (DESCRIBE): _____

ESTIMATED RIGOR MORTIS:
☐ COMPLETE ☐ PARTIAL ☐ NONE
☐ ARMS/HANDS ☐ LEGS/FEET ☐ HEAD
☐ RIGOR CONSISTENT WITH POSITION DECEDENT FOUND IN

ESTIMATED LIVOR MORTIS:
☐ UNFIXED (LIVOR AREA TURNS WHITE THEN BACK TO PINK/PURPLE IF TOUCHED)
☐ FIXED (LIVOR AREA STAYS PINK/PURPLE IF TOUCHED)
LOCATIONS: _____
☐ LIVOR CONSISTENT WITH POSITION DECEDENT FOUND IN & GRAVITY

PUTRIFACTION:
☐ ODOR ☐ SWELLING/BLOATING ☐ BLADDER/BOWELS EMPTIED
☐ DISCOLORATION OF ABDOMEN/GENITALS (DESCRIBE): _____
☐ MARBLING (LOCATIONS): _____
☐ PURGING (LOCATIONS): _____
☐ SKIN SLIPPAGE/BLISTERING (LOCATIONS): _____

OTHER:
☐ ADIPOCERE ☐ MUMMIFICATION ☐ CADAVERIC SPASM

NOTES: _____

INSECT & ANIMAL ACTIVITY:
☐ INSECTS ☐ DOMESTIC ANIMALS ☐ SCAVENGERS (OUTDOORS)
NOTES: _____

APPARENT WOUNDS:
☐ NONE VISIBLE ☐ GUNSHOT LOCATIONS: _____
☐ PUNCTURE ☐ SLICING ☐ STAB LOCATIONS: _____
☐ LACERATION ☐ ABRASION ☐ CONTUSION LOCATIONS: _____
☐ LIGATURE (LEAVE ON DECEDENT/ DO NOT CUT KNOT) LOCATIONS: _____
☐ BURNING ☐ IMMERSION IN WATER LOCATIONS: _____

*

DECEDENT MEDICAL HISTORY

PRESCRIPTION MEDICATIONS FOUND:

MEDICATION	DOSAGE	PRESCRIBED BY	DATE PRESCRIBED	PILLSREMAINING/PILLS PRESCRIBED

All Officers: Medications May Be Listed Above or the Bottle Labels May Be Photographed (Photograph All Sides of Labels)

ILLEGAL DRUGS FOUND:

All Officers: All Illegal Drugs Must Be Listed & Seized per Department SOP

KNOWN MEDICAL CONDITIONS:

All Officers: Known Medical Conditions Can Be Determined by Speaking with Family Members or Physicians Listed on Medications. If No Physician is Listed on Medications Contact Pharmacy on Medications & Ascertain the Prescribing Physician to Make Contact.

PHYSICIAN INFORMATION:

PHYSICIAN NAME	PHONE NUMBER	DATE LAST SEEN

NATURAL DEATH SCENES DECEDENT REMOVAL

IF:
Physician Contacted
&
Will Sign Death Certificate As Natural Causes
(DO NOT CONTACT OCME)

Physician Name: _____

Physician Phone: _____

IF:
Physician Cannot Be Contacted
Or
Physician Will Not Sign Death Certificate

Contact Medical Examiner's Office

M.E. / Investigators Name: _____

M.E. / Investigators Phone Number: _____

Date/Time: _____

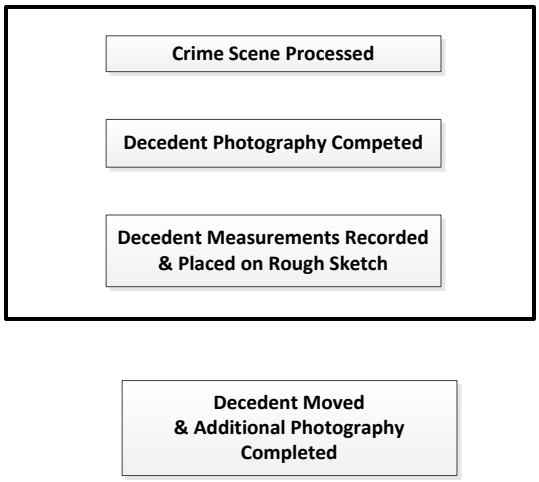
NON-NATURAL DEATH SCENES DECEDENT REMOVAL

THIS PORTION OF THE DEATH SCENE CHECKLIST IS COMPLETED BY FORENSIC UNIT INVESTIGATIONS / PERSONNEL ONLY

NON-NATURAL DEATHS ARE DEFINED AS FOLLOWS:

- **HOMICIDE**
- **SUICIDE**
- **SUSPICIOUS DEATH:**
  - **Undetermined Cause**
  - **Any Visible Injury or Trauma**
  - **Fire**
  - **Forced Entry (Not By 1st Responders)**
  - **Overdose**
  - **Accident (Non Motor Vehicle)**
  - **Other Burning or Immersion in Water**
- **CHILD DEATH/INDIVIDUAL UNDER 30 YEARS OLD**
- **ANY DEATH INVOLVING UNIVERSITY STUDENT**

NOTIFICATION OF THE FORENSIC UNIT POINT OF CONTACT IS REQUIRED IN ALL CASES LISTED ABOVE



M.E Name: _____
M.E. Phone: _____
Autopsy Date: _____

Funeral Home

Removal Contact: _____
Transport Time: _____

ADDITIONAL EVIDENCE RELATED TO VICTIM

SUICIDE NOTE:	☐ YES	☐ NO	☐ N/A	***PHOTOGRAPH NOTE & SEIZE AS EVIDENCE***
PRIMER RESIDUE:	☐ YES	☐ NO	☐ N/A	***PR KITS WILL BE TAKEN AT SCENE PER OCME***
LIGATURE:	☐ YES	☐ NO	☐ N/A	***PHOTOGRAPH & LEAVE ON VICTIM (MARK ENDS)**
HANDS BAGGED:	☐ YES	☐ NO	TIME: _____	
FEET BAGGED:	☐ YES	☐ NO	TIME: _____	

Naloxone Reporting Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

MADISON COUNTY SHERIFF'S OFFICE

Overdose Reversal and Naloxone Administration Reporting Form

Date of Incident: _____ **Time of Incident:** _____ **Case Number:** _____

Deputies Name: _____ **Badge #:** _____

Incident Location (Select One):

☐ Private Residence
☐ Hotel/Motel
☐ Sidewalk/Street
☐ Nursing home/assisted living
☐ School _____
☐ Business _____ Type of business _____
☐ Other _____

Physical Clues that made you administer naloxone (Select all that apply):

☐ Person looked blue
☐ Person had stopped breathing
☐ Person did not respond to sternal rub or painful stimuli
☐ Drugs or drug paraphernalia at scene
☐ Known history of drug use
☐ Other _____

What drugs were present on scene or suspected? _____
_____

Did someone administer naloxone before you arrived? ___ No ___ Yes, how many doses? _____

Were bystanders at the scene when you arrived? ___ No ___ Yes

How much naloxone was administered? ___ One dose ___ Two Doses ___ Other _____

How long do you believe it took to work? _____

What happened after you gave the person naloxone? (Select all that apply)

☐ Person woke up from overdose
☐ Person vomited
☐ Person went to the hospital. Which hospital? _____
☐ Person did not wake up from overdose
☐ Person died
☐ Other _____

Was an arrest made? ___ No ___ Yes

Victim's race:

☐ White
☐ Black
☐ Asian/Pacific Islander
☐ American Indian/Alaskan Native
☐ Unknown

Victim's gender:

☐ Male
☐ Female
☐ Unknown

Did you have any problems with your EVZIO Auto-Injector kit? ___ No ___ Yes, describe
_____

Other comments, notes or questions (Optional): _____
_____
_____
_____

Reviewed by: _____ Date: _____
Supervisor

Once this form is completed, please turn in to the EVZIO Auto-Injector Coordinator.

SUPERVISORS REPORT OF EMPLOYEE ACCIDENT.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Supervisor's Report of Injury

(Please Print – Please complete and return to Finance Department with Employee's Report of Injury and Accident Witness Statement)

ACCIDENT INFORMATION		
Supervisor's Name:		Supervisor's Telephone No:
Location where accident occurred:		County Premises: ☐ Yes ☐ No Job Site: ☐ Yes ☐ No
Who was injured:	☐ Employee ☐ Non-Employee	Time of Accident ☐ am ☐ pm
Department normally assigned to:	What property/equipment was damaged?	
Date Accident Was Reported to Supervisor: / /		Investigation Required: ☐ Yes ☐ No
Were Safeguards or Safety Equipment Provided: Provided: ☐ Yes ☐ No Utilized: ☐ Yes ☐ No		
Date of Incapacity: / /	Has Employed Returned to Work: ☐ Yes ☐ No	Modified Duty Required: ☐ Yes ☐ No
Witnesses:		

What was the employee doing when the accident occurred? Describe the activity as well as the tools, equipment, or material that the was using. Examples: "climbing a ladder while carrying materials".

What happened? Describe how the injury occurred. Examples: "when ladder slipped on wet floor, employee fell 20 feet".

What was the injury or illness? Describe the part of the body that was affected and how it was affected. Example: "strained lower back".

What object or substance directly harmed employee? Example: "concrete floor".

What can be done to prevent a reoccurrence?

_____ _____

Supervisor's Signature Date

EMPLOYEE ACCIDENT REPORT.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Employee's Report of Injury

(Please Print – Please complete and return to Supervisor)

EMPLOYEE INFORMATION

Employee's Last Name:	First:	Middle:	❑ Male ❑ Female	Date of Birth: / /
Street Address:	Social Security Number:			Home Telephone No: ( )
PO Box:	City:	State:		ZIP Code:

ACCIDENT INFORMATION

Date of Accident: / /	Time of Accident:	Location of Accident:
Witnesses:		
Were you performing a part of the normal job duty: □ yes □ no	Report Prepared by (if different than the injured employee):	

What were you doing when the accident occurred? Describe the activity as well as the tools, equipment, or material that you was using. Examples: "climbing a ladder while carrying materials".

What happened? Describe how the injury occurred. Examples: "when ladder slipped on wet floor, I fell 20 feet".

What was the injury or illness? Describe the part of the body that was affected and how it was affected. Example: "strained lower back".

What object or substance directly harmed you? Example: "concrete floor".

What can be done to prevent a reoccurrence?

EMERGENCY MEDICAL TREATMENT □ YES □ NO (IF YES, PLEASE INDICATED WHERE)

Treated by: □ Madison Family Physicians □ Orange Family Physicians

Hospital: □ Culpeper Memorial □ Martha Jefferson □ University of Virginia

In accordance with Virginia State Law, I hereby authorize Virginia Association of Counties Group Self-Insurance Associations (VACoGSIA), the insurer, or their representatives to be furnished with any information or facts, including records, diagnosis, medical treatment and prognosis, estimates of disability, and recommendations for further treatment. This information is to be used for the sole purpose of evaluating and handling any claim, and assuring timely medical care as a result of the incident occurring on or about the above noted date for no other purpose, now or in the future. I also agree that photographic carbonless copy of this release shall be as valid as the original.

_____ _____

Employee's Signature *Date*

Report of Discriminatory Harassment.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

[Madison County Sheriff's Office]

Discrimination/Harassment Complaint Form

If you believe you have experienced discrimination, sexual harassment, retaliation for filing a complaint or for your participation in an investigation or treated in a way that violates the Respectful Workplace Policy, you are encouraged to file a complaint. Send completed forms to _____

Relevant policy information is listed on the last page of this form.

Complainant (Personal Information about You)

Complainant's Name: _____

Preferred Email: _____

Preferred Phone: _____

Work Address (including City and Zip): _____

Job Title: _____

Division/Agency: _____

Manager: _____

Respondent (Person Against Whom You are Filing the Complaint)

Respondent's Name: _____

Preferred Email: _____

Preferred Phone: _____

Work Address (including City and Zip): _____

Job Title: _____

Division/Agency: _____

Manager: _____

Information on Witnesses Who You Believe Can Support Your Complaint			
Witness Name	**Witness Job Title**	**Work Location**	**Witness Work Phone**

Additional witnesses may be listed on a separate sheet attached to this form.

External Complaint

Have you filed this complaint with any other governmental agency? _____ Yes _____ No

If yes, what agency? _____

If yes, what is the status of the complaint? _____

The Complaint

Date(s) of Complaint

Date harassment/discrimination began or occurred: _____

Most recent date of harassment/discrimination (if different from above): _____

Basis of Complaint

Check all that apply:

I experienced unwelcome conduct of a sexual nature. *(Sexual Harassment Prohibited Policy*)*

I experienced discrimination or discriminatory harassment* based on my *(check all that apply):*

- Race
- Color
- National Origin
- Limited English Proficiency
- Religion Creed
- Disability
- Marital Status
- Familial Status
- Age Sex
- Pregnancy
- Gender Identity Gender
- Expression Sexual
- Orientation Genetic
- Information Public
- Assistance Status
- Membership or Activity in a Local Human Rights Commission

I experienced harassment or disrespectful behavior, but it is not based on any of the protected characteristics listed above.

I experienced retaliation for filing a complaint or participating in an investigation.

**For more information about the policies under which complaints may be filed, see last page.*

Describe, in as much detail as possible, the conduct that you believe violates the Harassment and Discrimination Prohibited Policy, the Sexual Harassment Prohibited Policy, or the Respectful Workplace Policy. List dates, locations, names, and titles of people involved. Explain why you believe the conduct was based on the items checked in the "Basis of Complaint" section above. Use additional paper if needed and attach to this form. Attach any documents you believe may be relevant (emails, notes, texts, etc.).

Verification

This complaint is being filed based on my honest belief that I have been subjected to conduct in violation of the Harassment and Discrimination Prohibited Policy, the Sexual Harassment Prohibited Policy, or the Respectful Workplace Policy. I hereby certify that the information I have provided in this complaint is true, correct, and complete to the best of my knowledge.

Complainant's signature: _____ Date Signed: _____

Complaint Received by: _____ Date Signed: _____

Non-Retaliation Notice

Retaliation against any person who reports conduct under the Harassment and Discrimination Prohibited Policy, the Sexual Harassment Prohibited Policy, or the Respectful Workplace Policy is strictly prohibited and will not be tolerated. If you believe that you have been subjected to retaliation, you are encouraged to report such behavior.

Privacy Notice

MCSO is asking you to provide information in this complaint form which includes private and/or confidential information. MCSO is asking for this private/confidential information so that it can investigate and respond to allegations of harassment, discrimination, or disrespectful behavior. You are not legally required to provide this information. However, if you do not provide sufficient information, MCSO may not be able to properly investigate your complaint. The information you provide will be used by MCSO employees whose job assignments reasonably require access to the information.

Employee and Supervisor Injury Report.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Employee's Report of Injury

(Please Print – Please complete and return to Supervisor)

EMPLOYEE INFROMATION

Employee's Last Name:	First:	Middle:	☐ Male ☐ Female	Date of Birth: / /
Street Address:	Social Security Number:			Home Telephone No: ( )
PO Box:	City:		State:	ZIP Code:
Department:	Supervisor:			Job Title:

ACCIDENT INFORMATION

Date of Accident: / /	Time of Accident: ☐ am ☐ pm	Location of Accident:
Witnesses:		
Were you performing a part of the normal job duty: ☐ yes ☐ no		Report Prepared by (if different than the injured employee):

What were you doing when the accident occurred? Describe the activity as well as the tools, equipment, or material that you was using. Examples: "climbing a ladder while carrying materials".

What happened? Describe how the injury occurred. Examples: "when ladder slipped on wet floor, I fell 20 feet".

What was the injury or illness? Describe the part of the body that was affected and how it was affected. Example: "strained lower back".

What object or substance directly harmed you? Example: "concrete floor".

What can be done to prevent a reoccurrence?

EMERGENCY MEDICAL TREATMENT ☐ YES ☐ NO (IF YES, PLEASE INDICATED WHERE)

Treated by: ☐ Madison Family Physicians ☐ Orange Family Physicians

Hospital: ☐ Culpeper Memorial ☐ Martha Jefferson ☐ University of Virginia

In accordance with Virginia State Law, I hereby authorize Virginia Association of Counties Group Self-Insurance Associations (VACoGSIA), the insurer, or their representatives to be furnished with any information or facts, including records, diagnosis, medical treatment and prognosis, estimates of disability, and recommendations for further treatment. This information is to be used for the sole purpose of evaluating and handling any claim, and assuring timely medical care as a result of the incident occurring on or about the above noted date for no other purpose, now or in the future. I also agree that photographic carbonless copy of this release shall be as valid as the original.

Employee's Signature *Date*

Supervisor's Report of Injury

(Please Print – Please complete and return to Finance Department with Employee's Report of Injury and Accident Witness Statement)

ACCIDENT INFORMATION		
Supervisor's Name:		Supervisor's Telephone No:
Location where accident occurred:		County Premises: ☐ Yes ☐ No Job Site: ☐ Yes ☐ No
Who was injured:	☐ Employee ☐ Non-Employee	Time of Accident ☐ am ☐ pm
Department normally assigned to:	What property/equipment was damaged?	
Date Accident Was Reported to Supervisor: / /		Investigation Required: ☐ Yes ☐ No
Were Safeguards or Safety Equipment Provided:	Provided: ☐ Yes ☐ No	Utilized: ☐ Yes ☐ No
Date of Incapacity: / /	Has Employed Returned to Work: ☐ Yes ☐ No	Modified Duty Required: ☐ Yes ☐ No
Witnesses:		

What was the employee doing when the accident occurred? Describe the activity as well as the tools, equipment, or material that the was using. Examples: "climbing a ladder while carrying materials".

What happened? Describe how the injury occurred. Examples: "when ladder slipped on wet floor, employee fell 20 feet".

What was the injury or illness? Describe the part of the body that was affected and how it was affected. Example: "strained lower back".

What object or substance directly harmed employee? Example: "concrete floor".

What can be done to prevent a reoccurrence?

_____ _____

Supervisor's Signature Date

VA Madison County SO - Off Site Forensic Interview Protocol (2017).pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

OFF-SITE FORENSIC INTERVIEW PROTOCOL –MADISON COUNTY

The Madison County Department of Social Services ("DSS"), Madison County Sheriff's Office ("Sheriff's Office"), Madison County Commonwealth's Attorney ("Commonwealth's Attorney"), Foothills Child Advocacy Center ("Foothills"), Madison County Victim/Witness Program ("Victim/Witness") understand that forensic interviews create an environment that provides a child an opportunity to talk to a trained professional about what the child has experienced or knows about a concern of maltreatment. The purpose of a forensic interview is to obtain a statement from a child in a developmentally and culturally sensitive, unbiased and fact-finding manner that will support accurate and fair decision-making by the multidisciplinary team ("MDT") members involved in the criminal justice and child protection systems. Quality interviews involve an appropriate, child-focused setting; effective communication among MDT members; and legally sound interviewing techniques. In order to make forensic interviews accessible to more children who have been allegedly abused, Foothills will conduct courtesy forensic interviews at a designated space at the Commonwealth's Attorney's Office.

Acceptance Criteria:
Foothills will accept children for courtesy forensic interviews that are referred by DSS Child Protective Services ("CPS") or the Sheriff's Office and are alleged victims in CPS and/or Sheriff's Office investigations and who are under age 18 at the time of the interview and who are alleged victims of criminal sexual assault or physical abuse. On a case-by-case basis, and at the discretion of the CPS investigator, Sheriff's Office investigator, and Foothills Program Coordinator, interviews will be conducted by a Foothills Forensic Interviewer with alleged child victims of neglect, victims of Internet Crimes Against Children, children who are a witness to a crime, or siblings and other children in the home of the victim who are not identified as the alleged offender in the CPS or Sheriff's Office investigation.

Scheduling a Courtesy Forensic Interview:
The assigned CPS and Sheriff's Office investigator will first make contact with each other to decide on a time when both team members can be present at the interview. The CPS or Sheriff's Office investigator will make contact with the parent or guardian of the child to decide on a time that the parent/guardian or other designated person can bring the child to the appointment. A calendar showing available dates/times for the Forensic Interviewer is located on the www.foothillscac.org home page. To schedule a courtesy interview, the assigned CPS or Sheriff's Office investigator shall contact the Foothills Program Coordinator or Family Support Specialist by phone or email and send a copy of the CPS or police report by email or fax. The assigned CPS or Sheriff's Office investigator will reserve the forensic interview room by calling or emailing the Commonwealth Attorney's Office. If time allows, FCAC will send a FCAC brochure to the parent.

Family Support/Advocacy:
A Family Support Specialist from Foothills will provide education and support to the non-offending caretaker when available, and will coordinate with CPS and Victim/Witness on referring the family for services. The Family Support Specialist will provide on-going support for the child and non-offending caretaker and will help the non-offending caretaker overcome any barriers to participating in mental health services. If a Family Support Specialist from Foothills cannot be present during the forensic interview appointment, Foothills will request that the Madison County Victim/Witness Director be present at the appointment.

The Child Forensic Interview
The interview will be legally sound, non-duplicative, non-leading, and developmentally appropriate. The Forensic Interviewer will be trained in one of the nationally recognized forensic interview protocols. The

assigned CPS worker and/or the detective will be present to observe the interview. Non-offending caretakers will not be allowed in the interview room during an interview. Alleged offenders will not be allowed in the courtesy interview building during the time of the child's interview.

Recording:
The interview will be audio and video recorded, pursuant to 22 VAC 40-705-80(B)(1). Recording the forensic interview is intended to prevent the MDT from needing to re-interview the child. Investigators will each bring their own flash drive for downloading the audio/video recorded interview. No copies of interviews will be stored on FCAC's laptop or recording equipment.

Hours of Operation:
A Foothills Forensic Interviewer will be available Monday through Friday from 9 a.m. to 6 p.m. In some cases, at the discretion of the Interviewer, the Sheriff's Office investigator, CPS investigator, and the Commonwealth's Attorney, a forensic interview appointment may last longer than the normal hours of operation.

MDT Case Review:
Cases subject to a forensic interview under this protocol may be discussed by the Madison County MDT, subject to the confidentiality requirements in the MDT memorandum of agreement.

ENDORSEMENTS:

Commonwealth's Attorney's Office for County of Madison

By: _____ Date: 5/1/17
Title: Commonwealth's Attorney

Madison County Sheriff's Office

By: _____ Date: 5-16-17
Title: Sheriff

Madison County Department of social services

By: Valerie Ward Date: 5/16/17
Title: Director

Madison County Victim Witness Program

By: _____ Date: 5-16-17
Title: Director

Foothills Child Advocacy Center

By: _____ Date: 5-18-17
Title: Executive Director

Rappahannock Rapidan Community Services MOU.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

d

COOPERATIVE AGREEMENT

between

Rappahannock Rapidan Community Services

and the

Community Services Area Criminal Justice, Law Enforcement, and Fire Department Agencies

The parties to this Cooperative Agreement (the "Agreement") are:

collectively referred to as the Partner Agencies.

WHEREAS, the Rappahannock Rapidan Crisis Intervention Team Project (the "CIT Project") is an innovative and collaborative effort between the Partner Agencies and the National Alliance on Mental Illness – Piedmont ("NAMI-Piedmont"); and the community; and

WHEREAS, the CIT Project is designed to effectively respond to individuals in psychiatric crisis, reduce the number of arrests and incarcerations for non-violent offenses by people with mental illness, enhance safety for all involved in a crisis situation, and strengthen the relationship between the Partner Agencies and the community; and

WHEREAS, an important component of the CIT Project is the development and implementation of CIT training for Criminal Justice, Police Department, Sheriff and Fire Department personnel that promotes techniques for dealing with individuals in mental illness or substance abuse crisis; and

WHEREAS, the CIT Project also has as goals (i) the establishment of a framework for data collection, research, and evaluation to support improved and consistent service delivery, effective use of resources and to enhance quality of care and (ii) the formation of a receiving center that is able to assess, triage, and stabilize persons in crisis.

NOW, THEREFORE, the Partner Agencies agree as follows:

I. TRAINING

The Partner Agencies agree to:

A. Collaboratively plan, develop, staff and implement CIT trainings to include a 40-hour basic class, advanced CIT training, train-the-trainer training, training for communication officers, and other mutually agreed-upon trainings.

B. Commit the necessary staff and personnel resources for the trainings.

C. Whenever possible, contribute to the costs of the trainings including supplies, facilities or other identified needs.

D. Work cooperatively with the Virginia Department of Criminal Justice Services to ensure that the training curriculum is approved for Department certified in-service training credits for law enforcement officers.

E. Assess and track within each Partner Agency the effectiveness of the trainings.

F. Meet at least annually to discuss changes to the curriculum or additional trainings that may be required or would enhance the CIT Project.

II. FUNDING

The Partner Agencies agree to pursue funding opportunities, including grants, outside funding sources, and other opportunities identified by the Partner Agencies, NAMI-Piedmont and the community.

The Partner Agencies agree to work collaboratively on a method to fund a CIT Coordinator, established under a separate agreement.

III. DATA COLLECTION

The Partner Agencies agree to identify desired goals, relevant sources of data collection and tracking and share data among the Partner Agencies to the extent permitted by federal, state and local laws and regulations relating to confidentiality.

IV. MEETINGS

The Partner Agencies agree to participate in regularly scheduled meetings to address CIT leadership, training, stakeholders, needs of the community and consumers, and other identified topics.

Overall project leadership is managed by the CIT Steering Committee comprised of representatives of all Partner Agencies providing supervision of the CIT Coordinator.

V. ONSITE COLLABORATION

The Partner Agencies agree to collaborate on scene. This will include CIT trained responders identifying themselves as such and offering consultation and guidance, as appropriate. When two or more CIT responders are onsite, they will offer coordination to facilitate an effective intervention for the consumer and to locate appropriate community resources to assist with identified needs.

VI. CRISIS STABILIZATION RECEIVING CENTER

The Partner Agencies agree to participate in developing and staffing a community crisis stabilization receiving center, as funding permits.

VII. AMENDMENT OR TERMINATION

The Partner Agencies agree to meet annually to discuss any necessary modifications to this Agreement. No amendment shall become effective unless reduced to writing signed by each of the Partner Agencies.

In the event that any Partner Agency desires to terminate its participation in the CIT Program, that Partner Agency shall provide the other Partner Agencies with 30 days prior written notice. The remaining Partner Agencies shall meet to determine whether to continue participation in the CIT Program or to terminate the Program.

VIII. TERM

This Agreement shall become effective upon execution by all Partner Agencies and shall be in effect for an initial term of one year. This Agreement shall automatically renew for additional one-year terms provided that the Partner Agencies meet annually as required by paragraph VII above to review the Agreement or unless terminated by the action of the Partner Agencies.

IX. CONFIDENTIALITY

The Partner Agencies and their agents, servants and employees shall comply with all federal, state and local laws and regulations relating to confidentiality, particularly the confidentiality of protected health information.

X. INTERPRETATION

Nothing in this Agreement shall be interpreted in such a manner that the interpretation would hinder or impede any Partner Agency in enforcing the laws, rules and regulations of the Commonwealth of Virginia or of jurisdictions within this region.

IN WITNESS WHEREOF, the Partner Agencies hereby execute this Agreement.

Warrenton Police Department

1/8/15

Louis A. Battle
Chief of Police

Rappahannock Rapidan Community Services Board

Brian Duncan
Executive Director
Date: 2/4/15

Culpeper County Sheriff's Office

Scott H. Jenkins
Sheriff
Date: 1-22-15

Culpeper Police Department

Chris R. Jenkins
Chief of Police
Date: 1-9-15

Orange County Sheriff's Office

Mark A. Amos
Sheriff
Date: 2/4/15

Germanna Community College Police

Craig Branch
Chief of Police
Date: 1/23/15

Rappahannock County Sheriff's Office

Connie Smith
Sheriff
Date: 1/23/15

Lord Fairfax Community College Police Department

Robert Marshall
Chief of Police
Date: 1/23/2015

Town of Orange Police Department

James L. Fenwick
Chief of Police
Date: 1-22-2015

Madison County Sheriff's Office

Erik Weaver
Sheriff
Date: 1/22/2015

Town of Remington Police Department

Charles Proffitt
Chief of Police
Date: 1-12-15

Northwestern Regional Adult Detention Center

James F. Whitley
Superintendent
Date: 1/22/15

Virginia State Police

Capt. Todd M Taylor for WSF
W. Steven Flaherty
Superintendent
Date: 1-9-15

Fauquier County Sheriff's Office

Robert P. Mosier
Sheriff
Date: 25 Feb 2016

Central Virginia Regional Jail

Frank Dyer
Superintendent
Date: 1-11-16

Sample Lineup Case Information Sheet.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

THIS PAGE OF THE FORM **MUST NOT** BE SHOWN TO THE WITNESS

LINE-UP CASE INFORMATION SHEET

Complaint or Case Report #:_____ Crime Date & Location: _____

Line-up Date: _____Time: _____ Location: _____

Crime Committed: _____Witness' Name: _____

Was Witness Transported? Yes □ No □

Transporting Officer: _____

Rank: _____ Command: _____ ID #: _____

Line-up Administrator: _____

Rank: _____ Command: _____ ID #: _____

Investigating Officer: _____

Rank: _____ Command: _____ ID #: _____

Security Officer: _____

Rank: _____ Command: _____ ID #: _____

Asst. District Attorney Present? Yes □ No □

Name of ADA: _____ Phone #: _____

Interpreter Present? Yes □ No □ Name: _____

Was the procedure video recorded? Video Only □ Audio & Video □ Audio Only □ No □

Line-up photograph taken? Yes □ No □ Witness initialed? Yes □ No □

Position	Name	Number Held	Age	Height	Weight
1					
2					
3					
4					
5					
6					

Suspect's name:_____ D.O.B. _____ Position:_____

Comments: _____

_____

Signature of Administrator: _____ Date: _____

Rappahannock Rapidan MOU re Transfer of Custody.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

d

Rappahannock Rapidan Crisis Intervention Team Assessment Center (CITAC)

A Program of Rappahannock Rapidan Community Services

Memorandum of Agreement – Transfer of Custody Protocol Between:

Rappahannock Rapidan Community Services
Orange County Sheriff's Department
Culpeper County Sheriff's Department
Madison County Sheriff's Department
Fauquier County Sheriff's Office
Remington Police Department
Germanna Community College Police Dept.
Lord Fairfax Community College
Town of Orange Police Department
Town of Culpeper Police Department
Rappahannock County Sheriff's Department
Town of Warrenton Police Department
Virginia State Police
Gordonsville Police Department

PURPOSE:

To establish the understanding of protocols and procedures as necessary to affect a transfer of custody for individuals held under an Emergency Custody Order by participating law enforcement agencies of the Rappahannock Rapidan Crisis Intervention Team (RRCIT) to the RRCS Crisis Intervention Team Assessment Center's contracted security located in Culpeper.

STATUTORY BASE:

The Code of Virginia establishes Rappahannock Rapidan Community Services (RRCS) as the local public behavioral health authority and establishes the powers and authority of Community Services Boards (Sections 37.2-500, et seq.) These include the responsibility to coordinate services related to the involuntary commitment process.

The Code of Virginia has established:
Orange County Sheriff's Department
Culpeper County Sheriff's Department
Madison County Sheriff's Department
Fauquier County Sheriff's Office
Remington Police Department
Germanna Community College
Lord Fairfax Community College
Town of Orange Police Department
Town of Culpeper Police Department
Rappahannock County Sheriff's Department
Town of Warrenton Police Department
Virginia State Police
Gordonsville Police Department

(collectively, law-enforcement agencies) through Sections 15.2-1600 et seq. and 15.2-1700 et seq., and Title 52 as provided through general law. The duties of the law enforcement agencies descried in the statute include authorization to initiate Emergency Custody Orders based on probable cause or to serve such orders issued by the Office of the Magistrate, and to provide transportation of individuals subject to such order to a location appropriate for the completion of an evaluation as required by Code of Virginia Section 37.2-808.

The Code of Virginia, Section 37.2-808 subsection E, permits the law enforcement agency providing such transportation to transfer custody of such individual to the facility in which the required evaluation will be completed. This subsection requires that the facility be licensed for, and capable of providing the requisite level of security to protect the person and others from harm. The subsection also requires the facility to enter into an agreement with law-enforcement agencies, setting forth the terms and conditions under which it will accept a transfer of custody.

The Rappahannock Rapidan CIT Assessment Center (CITAC) is located at 610 Laurel Street (second level) adjacent to UVA/Novant Culpeper Medical Center. The CITAC is licensed by the Virginia Department of Behavioral Health to serve as the areas regional evaluation center for individuals requiring evaluation for involuntary hospitalization during its posted

hours of operation. Medical clearances, if required, will be provided by UVA/Novant Culpeper Medical Center prior to admission to State or Private psychiatric facilities.

TRANSFER OF CUSTODY MEMORANDUM OF AGREEMENT

The Code of Virginia, Section 8.01-293 subsection 2, authorizes the execution of civil process by "any person of age 18 or older and who is not party or otherwise interested in the subject matter in controversy." This Section further states that the terms "officer" or "sheriff", in any section of the Code referencing "persons authorized to make, return or do any other act relating to service of process, such term shall be deemed to refer to any person authorized by this section to serve process". This authorization is further addressed in Section 8.01-295.

RESPONSIBILITIES OF EACH PARTY:

Pursuant to the stated purpose of this agreement, the agencies entering into this agreement shall fulfill the following responsibilities and procedures:

RESPONSIBLITIES DURING THE ECO PROCESS:

In the event of a law-enforcement officer initiated ECO or Magistrate issued ECO which is executed by an Officer in the community:

1. The initiating/executing law enforcement agency will contact RRCS/Access Emergency Services at 540-825-5656 to determine availability at the CIT Assessment Center (CITAC) site to accept a transfer of custody. Law enforcement will provide, to the greatest extent possible, the name, date of birth and other available information regarding the respondent.
2. Concurrently:
    a. As staffing permits, A Virginia Certified Pre-Admission Screener from RRCS will be available at the CITAC to conduct the evaluation and any other necessary services pursuant to the relevant sections of Virginia Code and policies of the Board. The CITAC will typically be open from: Monday thru Friday – 9:00 am to 11:30 pm and Saturday and Sunday from 1:00 pm to 12:00 pm.
    b. The Officer shall provide transportation to the individual to the CIT Assessment Center (CITAC). Officers will enter the Center through the designated entrance and inform the security officer of their arrival.
3. Once inside the secure area at the CITAC, or other treatment room as designated by the RRCS ES Clinician or CITAC Security, the Security Officer assigned to the CITAC, the ES Clinician, and the Law Enforcement Officer will evaluate the ability to provide the level of security for the individual based on assessment of need, activity level, known history of aggression and any other factors deemed necessary.
4. Determination based on this evaluation:
    a. Upon favorable determination of their present ability, the Security Officer assigned to the CITAC will accept the transfer of custody, by signatures of the authorized security officer and law-enforcement officer on a transfer of custody form designated for this purpose. This form shall include the date and time of execution for any law-enforcement officer initiated ECO, or shall be attached to the ECO paperwork if issued by a Magistrate.
    b. Upon the determination that any factor or combination of factors indicates the level of security required may exceed the facility's ability at that time, the security officer assigned to the CITAC will advise the law enforcement officer(s) of those factors and request that they maintain custody of the ECO until such time as the factors impeding security are resolved or the ECO concludes.
5. Upon completion of a transfer of custody the law enforcement officers are released to return to services. However, CITAC and RRCS reserve the right to request the return of law enforcement officers at any time during the duration of the ECO, if the security officer or RRCS ES clinician determine that changes in the overall situation have occurred which warrant such return.

In the event that an ECO is issued by the Magistrate when the respondent is already located within the CITAC facility:

1. Upon issuance of such an ECO:
    a. CITAC security will collaborate with the law enforcement agency executing the ECO to determine whether a transfer of custody is practicable.

b. Should transfer of custody be appropriate and upon completion of the transfer of custody form, the law enforcement agency is released. However, as in section 5 above, CITAC and RRCS reserve the right to request the law-enforcement agency to respond to take or resume custody of the respondent at any time during the duration of the ECO upon determining that such return is warranted.

RESPONSIBILITIES IN THE EVENT THAT THE RESPONDENT IS RELEASED FROM THE ECO:

Once an ECO has be initiated, regardless of its initiation by law enforcement or Magistrate issue, prior to its expiration, it may only be released by the CSB ES Certified Pre-Admission Screener, following their evaluation, and upon finding that the individual does not meet the criteria for recommendation of a Temporary Detention Order (TDO).

In the event that the RRCS ES Clinician makes that finding that the respondent of the ECO should be released:

1. When no transfer of custody, the RRCS ES Clinician will release the ECO and the law-enforcement officer(s) by signature on the ECO or transfer of custody paperwork as appropriate.
2. In the event a transfer of custody had already occurred:
    a. The RRCS ES Clinician will release the ECO by signature on the ECO paperwork and/or the Transfer of Custody form as appropriate.
    b. If applicable, the RRCS ES Clinician will transmit the completed ECO paperwork by mail or facsimile to the Court designated by the issuing Magistrate pursuant to the Code of Virginia Section 37.2-808 subsection C.
    c. When other transportation options are not available, the law enforcement agency that initiated the ECO will return to the CITAC and provide transportation for the individual back to their home or the location where the respondent was taken into custody.

RESPONSIBILITIES DURING THE TDO PROCESS:

If contracted transportation is not available, the appropriate law enforcement agency will, upon receipt of the TDO paperwork from the Magistrate, serve the TDO and provide transportation of the respondent to the facility of temporary detention as identified on the TDO order.

FEES OR COSTS ASSOCIATED WITH THE ECO/TDO and CUSTODY PROCESSES:

Nothing herein shall be construed to obligate any law enforcement agency for the payment of any fees, expenses or damages incurred by RRCS or CITAC during the ECO/TDO or Transfer of Custody processes.

MODIFICATION OR TERMINATION OF THIS AGREEMENT:

This agreement will become effective immediately following the signature of all parties, and will be reviewed annually and renewed or modified as required. With the exception of changes required to comply with changes in Code or statute or based on funding available to continue CITAC operations, this agreement shall not be modified without unanimous agreement from all partner agencies OR 90 days written notice to all other parties prior to a party terminating its participation. Any modifications must maintain compliance with the Code of Virginia and governing regulations of the partner agencies.

This agreement shall be construed and interpreted pursuant to the laws of the Commonwealth of Virginia, without regard to its conflicts of law's provisions. Any disputes arising under this agreement shall only be brought in a Court of the Commonwealth. Nothing herein waives the sovereign immunity of state agencies or the Commonwealth of Virginia.

All parties hereby agree to hold each other harmless from any claims or causes of action arising pursuant to this agreement.

Brian Duncan, Executive Director RRCS

W. Stephen Flaherty, Virginia State Police Superintendent

Orange County Sheriff's Department

Town of Orange Police Department

Culpeper County Sheriff's Department

Town of Culpeper Police Department

Madison County Sheriff's Department

Rappahannock County Sheriff's Department

Robert P. Mosier / Robert P. Mosier 30 Dec 2016

Fauquier County Sheriff's Office

Town of Warrenton Police Department

Remington Police Department

Gordonsville Police Department

Germanna Community College Police Department

Lord Fairfax Community College

406 USDOT HAZMAT Identification Guidebook.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

A guidebook intended for use by first responders
during the initial phase of a transportation incident
involving hazardous materials/dangerous goods

2020
EMERGENCY RESPONSE GUIDEBOOK



U.S. Department of Transportation
Pipeline and Hazardous Materials Safety Administration

Transport Canada
Transports Canada

SCT
SECRETARÍA DE COMUNICACIONES Y TRANSPORTES

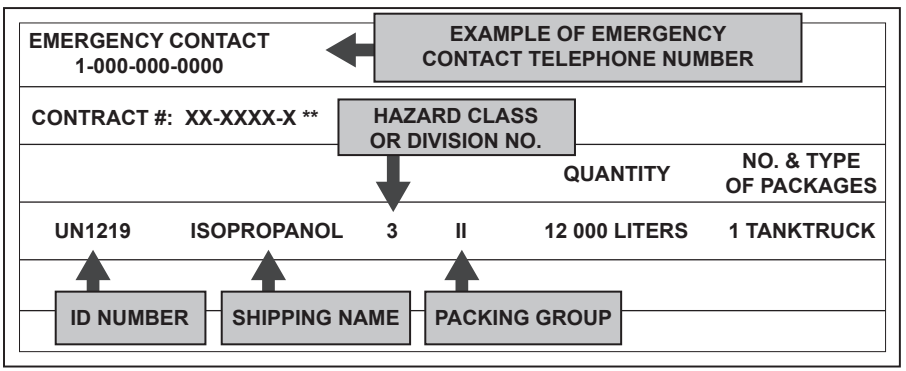
SHIPPING PAPERS (DOCUMENTS)

For the purpose of this guidebook, shipping documents and shipping papers are synonymous. Shipping papers provide vital information regarding the hazardous materials/dangerous goods to initiate protective actions. A consolidated version of the information found on shipping papers may be found as follows:

- Road – kept in the cab of a motor vehicle
- Rail – kept in possession of a crew member
- Aviation – kept in possession of the pilot or aircraft employees
- Marine – kept in a holder on the bridge of a vessel

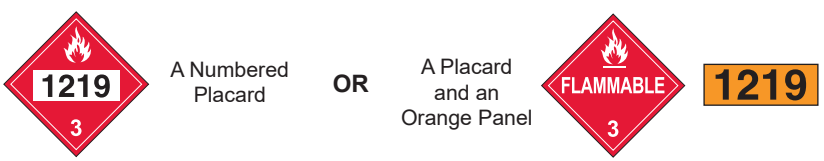
Information provided:

- 4-digit identification number, UN or NA (go to yellow pages)
- Proper shipping name (go to blue pages)
- Hazard class or division number of material
- Packing group
- Emergency response telephone number
- Information describing the hazards of the material (entered on or attached to the shipping paper)*



EXAMPLE OF PLACARD AND PANEL WITH ID NUMBER

The 4-digit ID Number may be shown on the diamond-shaped placard or on an adjacent orange panel displayed on the ends and sides of a cargo tank, vehicle or rail car.



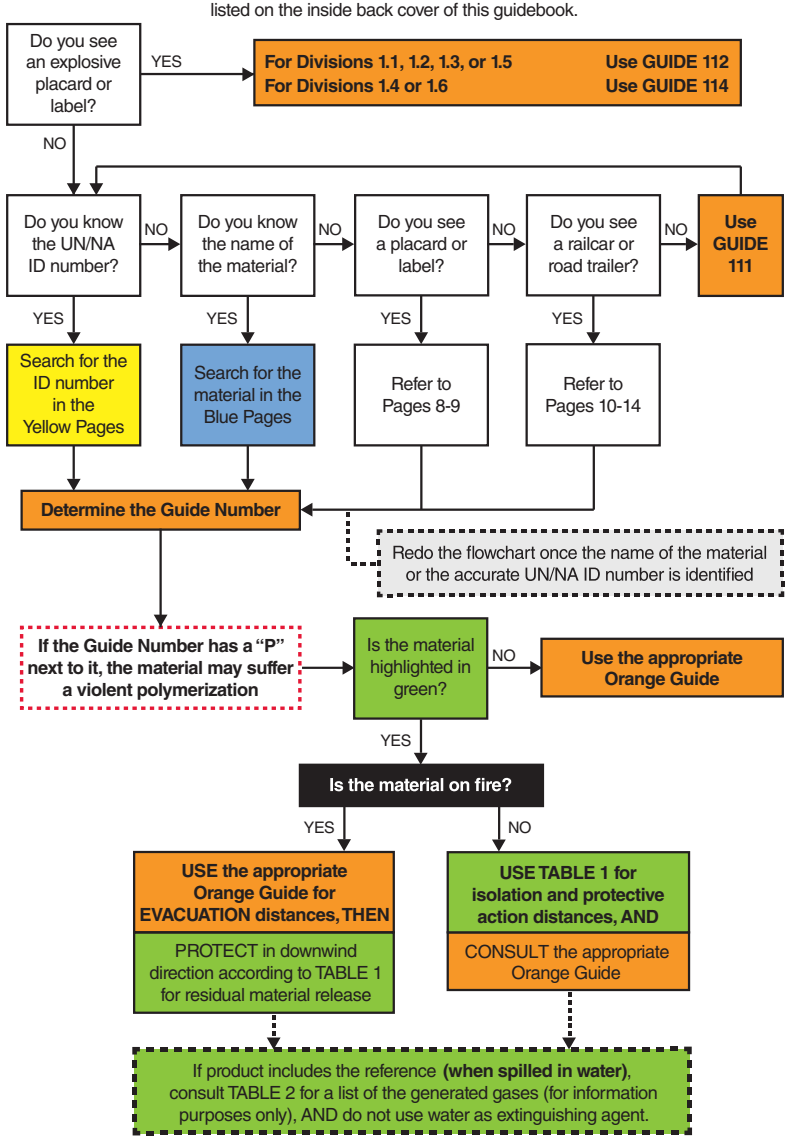
* In the United States, this requirement may be satisfied by attaching a guide from the ERG2020 to the shipping paper, or by having the entire guidebook available for reference.

** In the United States, a registration or contract number may be required on a shipping paper.

HOW TO USE THIS GUIDEBOOK

RESIST RUSHING IN!
APPROACH INCIDENT FROM UPWIND, AND UPHILL AND/OR UPSTREAM
STAY CLEAR OF ALL SPILLS, VAPORS, FUMES, SMOKE, AND POTENTIAL HAZARDS

WARNING: DO NOT USE THIS FLOWCHART if more than one hazardous material/dangerous good is involved. Immediately call the appropriate emergency response agency telephone number listed on the inside back cover of this guidebook.



BEFORE AN EMERGENCY - BECOME FAMILIAR WITH THIS GUIDEBOOK!

First responders must be trained in the use of this guidebook.

LOCAL EMERGENCY TELEPHONE NUMBERS

Please populate this page with emergency telephone numbers for local assistance:

HAZMAT CONTRACTORS

RAIL COMPANIES

FEDERAL/STATE/PROVINCIAL AGENCIES

OTHERS

TABLE OF CONTENTS

Shipping Papers (Documents) . . . . . Inside front cover
How to Use this Guidebook 1
Local Emergency Telephone Numbers 2
Safety Precautions 4
Notification and Request for Technical Information 5
Hazard Classification System 6
Introduction to the Table of Markings, Labels And Placards 7
Table of Markings, Labels, and Placards and Initial Response Guide to Use On-scene . . 8
Rail Car Identification Chart 10
Road Trailer Identification Chart 12
Globally Harmonized System of Classification and Labeling of Chemicals (GHS) 16
Hazard Identification Numbers Displayed On Some Intermodal Containers 18
Pipeline Transportation 22
ID Number Index (yellow pages) 28
Name of Material Index (blue pages) 92
Guides (orange pages) 156
Introduction to Green Tables 286
Protective Actions 289
Protective Action Decision Factors to Consider 291
Background on Table 1 – Initial Isolation and Protective Action Distances 292
Table 1 – Initial Isolation and Protective Action Distances 294
Table 2 – Water-Reactive Materials That Produce Toxic Gases 344
Table 3 – Initial Isolation and Protective Action Distances for Large Spills for Different Quantities of Six Common TIH (PIH in the US) Gases 350
ERG2020 User's Guide 354
Protective Clothing 360
Decontamination 362
Fire and Spill Control 363
BLEVE and Heat Induced Tear 365
BLEVE – Safety Precautions 366
Criminal or Terrorist Use of Chemical, Biological and Radiological Agents 368
Improvised Explosive Device (IED) Safe Stand-Off Distance 373
Glossary 375
Publication Data 386
Canada and United States National Response Centers 389
24-Hour Emergency Response Telephone Numbers 392

SAFETY PRECAUTIONS

RESIST RUSHING IN!

APPROACH CAUTIOUSLY FROM *UPWIND, UPHILL* AND/OR *UPSTREAM*:

- Stay clear of ***Vapor, Fumes, Smoke and Spills.***
- Keep vehicle at a safe distance from the scene.

SECURE THE SCENE:

- Isolate the area and protect yourself and others.

IDENTIFY THE HAZARDS USING ANY OF THE FOLLOWING:

- Placards
- Container labels
- Shipping papers
- Rail Car and Road Trailer Identification Chart
- Safety Data Sheets (SDS)
- Knowledge of persons on scene
- Consult applicable guide page

ASSESS THE SITUATION:

- Is there a fire, a spill or a leak?
- What are the weather conditions?
- What is the terrain like?
- Who/what is at risk: people, property or the environment?
- What actions should be taken – evacuation, shelter-in-place or dike?
- What resources (human and equipment) are required?
- What can be done immediately?

OBTAIN HELP:

- Advise your headquarters to notify responsible agencies and call for assistance from qualified personnel.

RESPOND:

- Enter only when wearing appropriate protective gear.
- Rescue attempts and protecting property must be weighed against you becoming part of the problem.
- Establish a command post and lines of communication.
- Continually reassess the situation and modify response accordingly.
- Consider safety of people in the immediate area first, including your own safety.

ABOVE ALL: Do not assume that gases or vapors are harmless because of lack of a smell – odorless gases or vapors may be harmful. Use **CAUTION** when handling empty containers because they may still present hazards until they are cleaned and purged of all residues.

NOTIFICATION AND REQUEST FOR TECHNICAL INFORMATION

Follow the steps outlined in your organization's standard operating procedures and/or local emergency response plan for obtaining qualified assistance. Generally, the notification sequence and requests for technical information beyond what is available in this guidebook should occur in the following order:

1. NOTIFY YOUR ORGANIZATION/AGENCY:

- Based on information provided, this will set in motion a series of events. Actions may range from dispatching additional trained personnel to the scene, to activating the local emergency response plan.
- Ensure that local fire and police departments have been notified.

2. CALL THE EMERGENCY RESPONSE TELEPHONE NUMBER ON THE SHIPPING PAPER

- If shipping paper is not available, use guidance under next section **"NATIONAL ASSISTANCE"**.

3. NATIONAL ASSISTANCE

- Contact the appropriate emergency response agency listed on the inside back cover of this guidebook.
- Provide as much information about the hazardous material/dangerous good and the nature of the incident.
- The agency will provide immediate advice on handling the early stages of the incident.
- The agency will also contact the shipper or manufacturer of the material for more detailed information if necessary.
- The agency will request on-scene assistance when necessary.

4. PROVIDE AS MUCH OF THE FOLLOWING INFORMATION AS POSSIBLE:

- Your name, call-back telephone number, fax number
- Location and nature of problem (spill, fire, etc.)
- Name and identification number of material(s) involved
- Shipper/consignee/point-of-origin
- Carrier name, rail car or truck number
- Container type and size
- Quantity of material transported/released
- Local conditions (weather, terrain)
- Proximity to schools, hospitals, waterways, etc.
- Injuries and exposures
- Local emergency services that have been notified

HAZARD CLASSIFICATION SYSTEM

The hazard class of hazardous materials/dangerous goods is indicated either by its class (or division) number or name. Placards are used to identify the class or division of a material. The hazard class or division number must be displayed in the lower corner of a placard and is required for both primary and subsidiary hazard classes and divisions, if applicable. For other than Class 7 placards, text indicating a hazard (for example, "CORROSIVE") is not required. Text is shown only in the U.S. The hazard class or division number and subsidiary hazard classes or division numbers placed in parentheses (when applicable), must appear on the shipping paper after each proper shipping name.

Class 1 - Explosives

Division 1.1	Explosives which have a mass explosion hazard
Division 1.2	Explosives which have a projection hazard but not a mass explosion hazard
Division 1.3	Explosives which have a fire hazard and either a minor blast hazard or a minor projection hazard or both, but not a mass explosion hazard
Division 1.4	Explosives which present no significant hazard
Division 1.5	Very insensitive explosives with a mass explosion hazard
Division 1.6	Extremely insensitive articles which do not have a mass explosion hazard

Class 2 - Gases

Division 2.1	Flammable gases
Division 2.2	Non-flammable, non-toxic* gases
Division 2.3	Toxic* gases

Class 3 - Flammable liquids (and Combustible liquids [U.S.])

Class 4 - Flammable solids; Substances liable to spontaneous combustion; Substances which, on contact with water, emit flammable gases

Division 4.1	Flammable solids, self-reactive substances and solid desensitized explosives
Division 4.2	Substances liable to spontaneous combustion
Division 4.3	Substances which in contact with water emit flammable gases

Class 5 - Oxidizing substances and Organic peroxides

Division 5.1	Oxidizing substances
Division 5.2	Organic peroxides

Class 6 - Toxic* substances and Infectious substances

Division 6.1	Toxic* substances
Division 6.2	Infectious substances

Class 7 - Radioactive materials

Class 8 - Corrosive substances

Class 9 - Miscellaneous hazardous materials/dangerous goods and articles

* The words "poison" or "poisonous" are synonymous with the word "toxic".

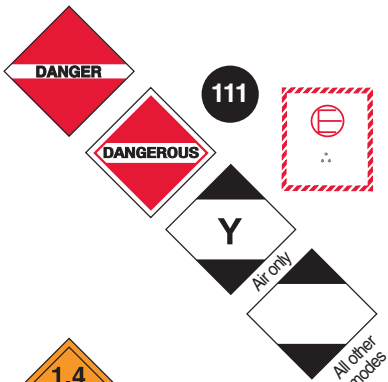
INTRODUCTION TO THE TABLE OF MARKINGS, LABELS AND PLACARDS

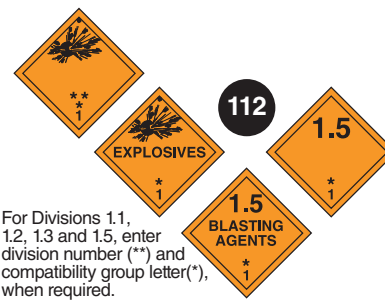
USE THIS TABLE ONLY WHEN THE ID NUMBER OR PROPER SHIPPING NAME IS NOT AVAILABLE.

The next two pages display the placards used on transport vehicles carrying hazardous materials/dangerous goods with the applicable reference GUIDE circled. Follow these steps:

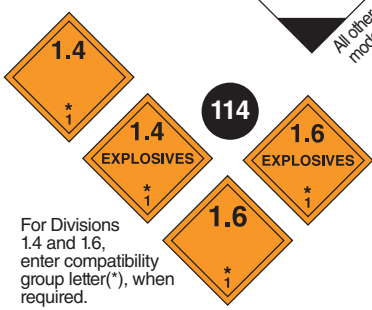
1. **Approach scene from upwind, uphill and/or upstream at a safe distance to safely identify and/or read the placard or orange panel. Use binoculars if available.**
2. **Match the vehicle placard(s) with one of the placards displayed on the next two pages.**
3. **Consult the circled guide number associated with the placard. Use that guide information for now. For example:**
   - Use GUIDE **127** for a FLAMMABLE (Class 3) placard 
   - Use GUIDE **153** for a CORROSIVE (Class 8) placard 
   - Use GUIDE **111** when the DANGER or DANGEROUS placard is displayed or the nature of the spilled, leaking or burning material is not known. Also use this GUIDE when the presence of hazardous materials/dangerous goods is suspected but no placards can be seen.

   If multiple placards point to more than one guide, initially use the most conservative guide (i.e., the guide requiring the greatest degree of protective actions).
4. **Guides associated with the placards provide the most significant risk and/or hazard information.**
5. **When specific information, such as ID number or proper shipping name, becomes available, the more specific Guide recommended for that material must be consulted.**
6. **A single asterisk (*) on orange placards represents an explosive's compatibility group letter. The asterisk must be replaced with the appropriate compatibility group letter. Refer to the Glossary (page 375).**
7. **Double asterisks (**) on orange placards represent the division of the explosive. The double asterisks must be replaced with the appropriate division number.**

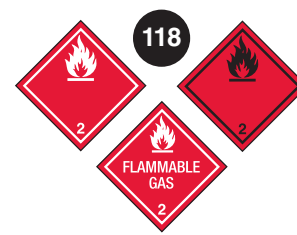


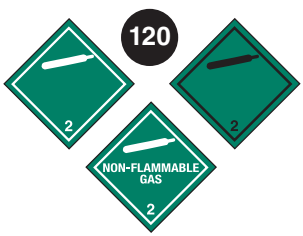


For Divisions 1.1, 1.2, 1.3 and 1.5, enter division number (**) and compatibility group letter(*), when required.



For Divisions 1.4 and 1.6, enter compatibility group letter(*), when required.



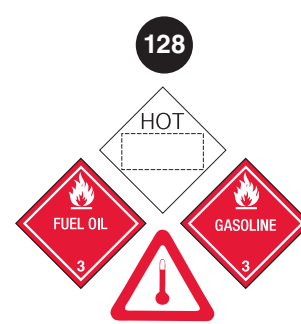










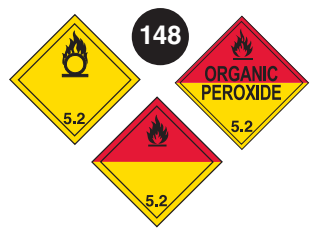



134
4
FLAMMABLE SOLID
4

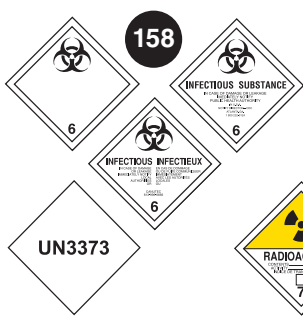

136
4
SPONTANEOUSLY COMBUSTIBLE
4

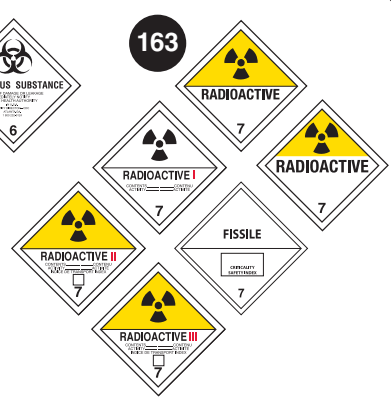

139
4
4
DANGEROUS WHEN WET
4

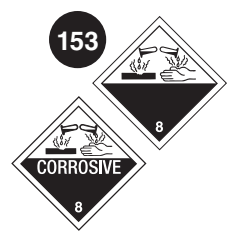

143
5.1
OXIDIZER
5.1

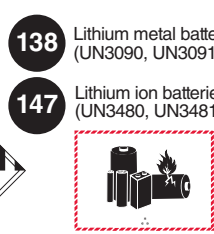

148
5.2
ORGANIC PEROXIDE
5.2
5.2

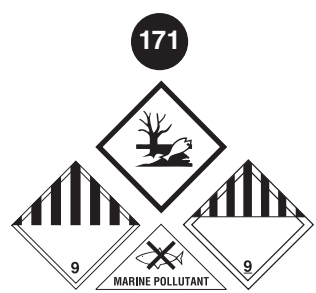

153
6
TOXIC
6
POISON
6
INHALATION HAZARD
6


158
6
INFECTIOUS SUBSTANCE
6
INFECTIOUS INFECTIEUX
6
UN3373


163
RADIOACTIVE
7
RADIOACTIVE I
7
RADIOACTIVE
7
RADIOACTIVE II
7
FISSILE
7
RADIOACTIVE III
7


153
8
CORROSIVE
8


138
Lithium metal batteries
(UN3090, UN3091)
147
Lithium ion batteries
(UN3480, UN3481)
9


171
9
MARINE POLLUTANT
9

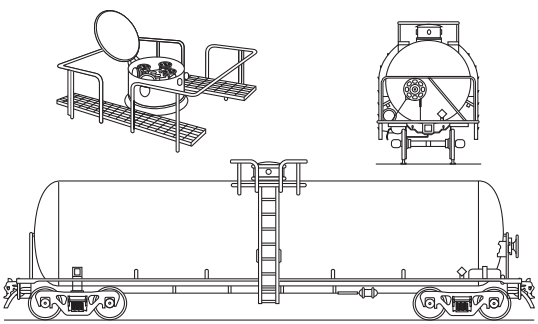
RAIL CAR IDENTIFICATION CHART

CAUTION: Emergency response personnel must be aware that rail tank cars vary widely in construction, fittings and purpose. Tank cars could transport products that may be solids, liquids or gases. The products may be under pressure. It is essential that products be identified by consulting shipping papers or train consist or contacting dispatch centers before emergency response is initiated. The information stenciled on the sides or ends of tank cars, as illustrated below, may be used to identify the product utilizing:

a. the commodity name shown;
b. the other information shown, especially reporting marks and car number which, when supplied to a dispatch center, will facilitate the identification of the product.

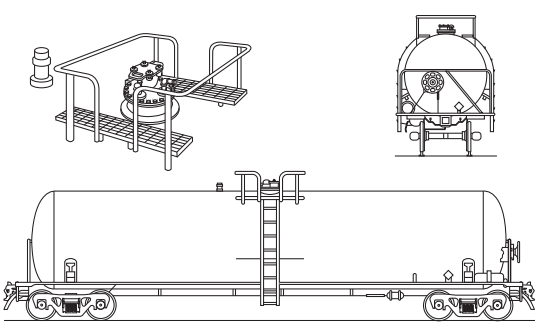
The recommended guides should be considered as last resort if the material cannot be identified by any other means.

117 Pressure tank car



- For flammable, non-flammable, toxic and/or liquefied compressed gases
- Protective housing
- No bottom fittings
- Pressures usually above 40 psi

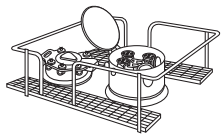
131 Non-pressure / low pressure tank car

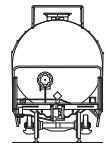


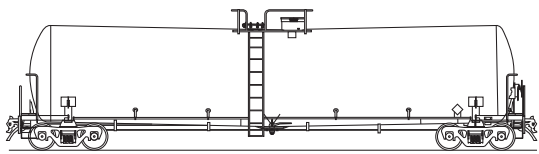
- Known as **general service tank car**
- For variety of hazardous and non-hazardous materials
- Fittings and valves normally visible at the top of the tank
- Some may have bottom outlet valve
- Pressures usually below 25 psi

RAIL CAR IDENTIFICATION CHART

128 Non-pressure / low pressure tank car (TC117, DOT117)

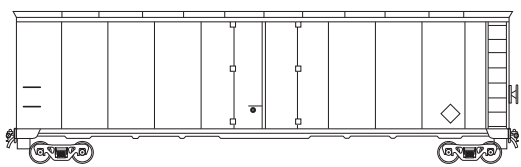






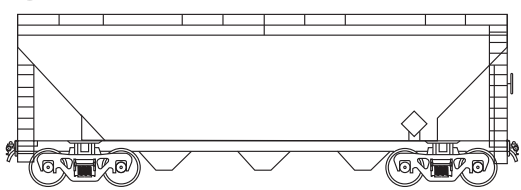
- For flammable liquids (e.g.,
- Petroleum crude oil, ethanol)
- Protective housing separate from manway
- Bottom outlet valve
- Pressures usually below 25 psi

111 Box car



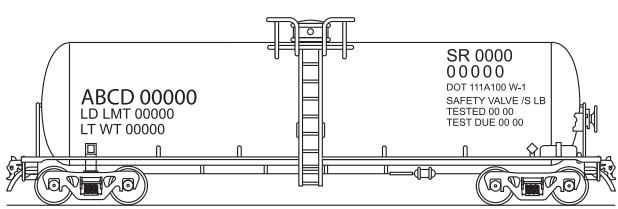
- For general freight that carry bulk or non-bulk packages
- May transport hazardous materials/dangerous goods in small packages or "tote bins"
- Single or double sliding door

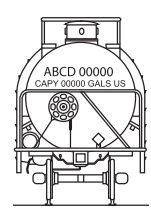
140 Hopper car



- For bulk commodities and bulk cargo (e.g., coal, ore, cement and solid granular materials)
- Bulk lading discharged by gravity through the hopper bottom doors when doors opened

COMMON MARKINGS ON RAIL CARS: reporting marks and car number, load limit (pounds or kilograms), empty weight of car, placard, tank qualification and pressure relief device information, car specification, and commodity name.





ROAD TRAILER IDENTIFICATION CHART

CAUTION: This chart depicts only the most general shapes of road trailers and cargo transport units. Emergency response personnel must be aware that there are many variations of road trailers, not illustrated below, that are used for shipping chemical products. Many intermodal tanks that transport liquids, solids, liquefied compressed gases, and refrigerated liquefied gases have similar silhouettes. The suggested guides are for the most hazardous products that may be transported in these trailer types.

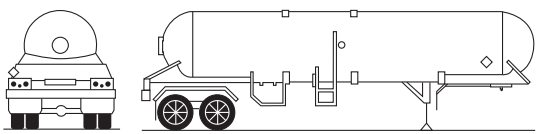
WARNING: Road trailers may be jacketed, the cross-section may look different than shown and external ring stiffeners would be invisible.

NOTE: An emergency shut-off valve is commonly found at the front of the tank, near the driver door.

The recommended guides should be considered as last resort if the material cannot be identified by any other means.

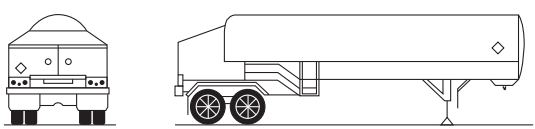
MAWP: Maximum Allowable Working Pressure.

117 MC331, TC331, SCT331



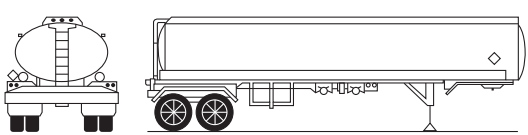
- For liquefied compressed gases (e.g., LPG, ammonia)
- Rounded heads
- Design pressure between 100-500 psi

117 MC338, TC338, SCT338, TC341, CGA341



- For refrigerated liquefied gases (cryogenic liquids)
- Similar to a "giant thermo-bottle"
- Fitting compartments located in a cabinet at the rear of the tank
- MAWP between 25-500 psi

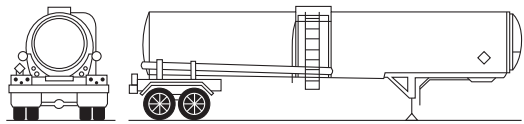
131 DOT406, TC406, SCT306, MC306, TC306



- For flammable liquids (e.g., gasoline, diesel)
- Elliptical cross-section
- Rollover protection at the top
- Bottom outlet valves
- MAWP between 3-15 psi

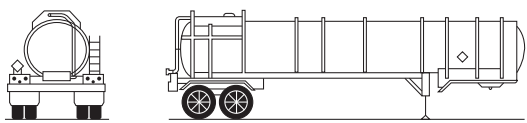
ROAD TRAILER IDENTIFICATION CHART

137 DOT407, TC407, SCT307, MC307, TC307



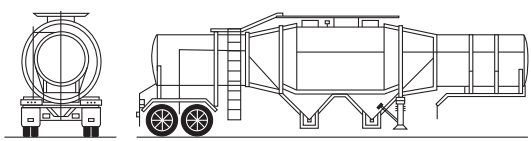
- For toxic, corrosive, and flammable liquids
- Circular cross-section
- May have external ring stiffeners
- MAWP of at least 25 psi

137 DOT412, TC412, SCT312, MC312, TC312



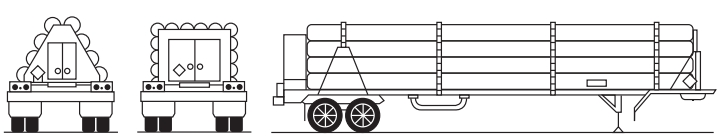
- Usually for corrosive liquids
- Circular cross-section
- External ring stiffeners
- Tank diameter is relatively small
- MAWP of at least 15 psi

112 TC423



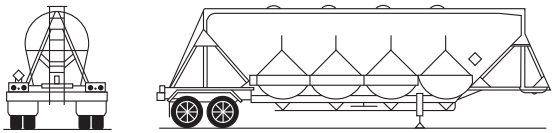
- For emulsion and water-gel explosives
- Hopper-style configuration
- MAWP between 5-15 psi

117 Compressed Gas/Tube Trailer

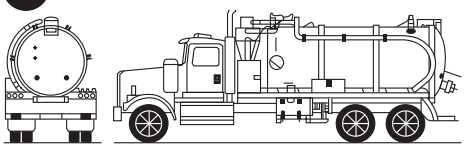


ROAD TRAILER IDENTIFICATION CHART

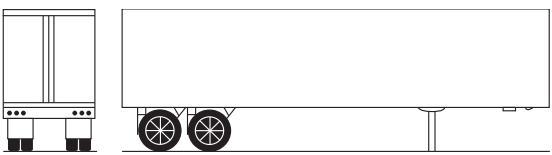
134 Dry Bulk Cargo Trailer



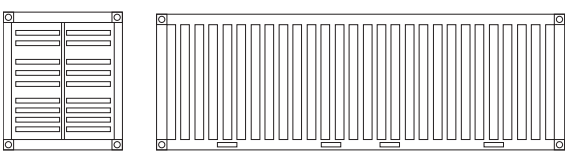
137 Vacuum Tanker



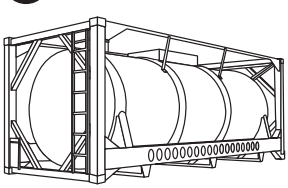
111 Mixed Cargo



111 Intermodal Freight Container



117 Intermodal Tank



NOTES

GLOBALLY HARMONIZED SYSTEM OF CLASSIFICATION AND LABELING OF CHEMICALS (GHS)

(May be found on means of containment during transport)

The Globally Harmonized System of Classification and Labeling of Chemicals (GHS) is an international guideline published by the United Nations. The GHS aims to harmonize the classification and labeling systems for all sectors involved in the life cycle of a chemical (production, storage, transport, workplace use, consumer use and presence in the environment).

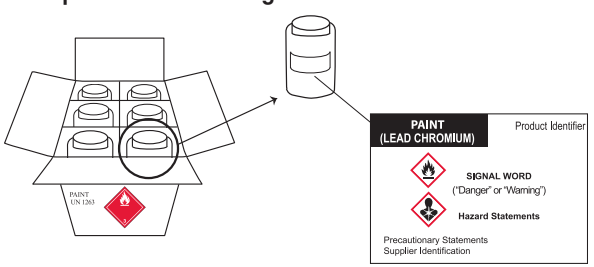
The GHS has nine symbols used to convey specific physical, health and environmental hazard information. These symbols are part of a pictogram that is diamond shaped and includes the GHS symbol in black on a white background with a red frame. The pictogram is part of the GHS label, which also includes the following information:

- **Signal word**
- **Hazard statement**
- **Precautionary statements**
- **Product identifier**
- **Supplier identification**

GHS pictograms are similar in shape to transport labels; however, transport labels have backgrounds of different colors.

The elements of the GHS that address signal words and hazard statements are not expected to be adopted in the transport sector. For substances and mixtures covered by the UN Recommendations on the Transport of Dangerous Goods, Model Regulations, the transport labels for physical hazards will have precedence. In transport, a GHS pictogram for the same (or lesser) hazard as the one reflected by the transport label or placard should not be present, but it could exist on the package.

Examples of GHS labeling:



Outer Packaging: Box with flammable liquid transport label

Inner Packaging: Plastic bottle with GHS hazard warning label

Single Packaging: 200 L (55 US gallons) drum with a flammable liquid transport label combined with GHS hazard warning label

In some cases, such as on drums or international bulk containers (IBCs), which must address information for all sectors, the GHS label may be found in addition to the required transport labels and placards. Both types of labels (GHS and transport) will differ in a way that will make them easy to identify during an emergency.

GHS Pictograms	Physical hazards	GHS Pictograms	Health and Environmental hazards
	Explosive; Self-reactive; Organic peroxide		Skin corrosion; Serious eye damage
	Flammable; Pyrophoric; Self-reactive; Organic peroxide; Self-heating; Emits flammable gases when in contact with water		Acute toxicity (harmful); Skin sensitizer; Irritant (skin and eye); Narcotic effect; Respiratory tract irritant; Hazardous to ozone layer (environment)
	Oxidizer		Respiratory sensitizer; Mutagen; Carcinogen; Reproductive toxicity; Target organ toxicity; Aspiration hazard
	Gas under pressure		Hazardous to aquatic environment
	Corrosive to metals		Acute toxicity (fatal or toxic)

HAZARD IDENTIFICATION NUMBERS DISPLAYED ON SOME INTERMODAL CONTAINERS

Hazard identification numbers, utilized under European and some South American regulations, may be found in the top half of an orange panel on some intermodal bulk containers. The 4-digit ID number is in the bottom half of the orange panel.



The hazard identification number in the top half of the orange panel consists of two or three digits. In general, the digits indicate the following hazards:

2 - Emission of gas due to pressure or chemical reaction

3 - Flammability of liquids (vapors) and gases or self-heating liquid

4 - Flammability of solids or self-heating solid

5 - Oxidizing (fire-intensifying) effect

6 - Toxicity or risk of infection

7 - Radioactivity

8 - Corrosivity

9 - Risk of spontaneous violent reaction

NOTE: The risk of spontaneous violent reaction within the meaning of digit 9 includes the possibility, due to the nature of a substance, of a risk of explosion, disintegration and polymerization reaction followed by the release of considerable heat or flammable and/or toxic gases.

- Doubling of a digit indicates an intensification of that particular hazard (i.e., 33, 66, 88).
- Where the hazard associated with a substance can be adequately indicated by a single digit, the digit is followed by a zero (i.e., 30, 40, 50).
- A hazard identification number prefixed by the letter “X” indicates that the substance will react dangerously with water (i.e., X88).

HAZARD IDENTIFICATION NUMBERS DISPLAYED ON SOME INTERMODAL CONTAINERS

The hazard identification numbers listed below have the following meanings:

20	Asphyxiant gas or gas with no subsidiary hazard
22	Refrigerated liquefied gas, asphyxiant
223	Refrigerated liquefied gas, flammable
225	Refrigerated liquefied gas, oxidizing (fire-intensifying)
23	Flammable gas
238	Gas, flammable corrosive
239	Flammable gas which can spontaneously lead to violent reaction
25	Oxidizing (fire-intensifying) gas
26	Toxic gas
263	Toxic gas, flammable
265	Toxic gas, oxidizing (fire-intensifying)
268	Toxic gas, corrosive
28	Gas, corrosive
30	Flammable liquid (flash-point between 23°C and 60°C, inclusive), or flammable liquid or solid in the molten state with a flash-point above 60°C, heated to a temperature equal to or above its flash point, or self-heating liquid
323	Flammable liquid which reacts with water, emitting flammable gases
X323	Flammable liquid which reacts dangerously with water, emitting flammable gases
33	Highly flammable liquid (flash-point below 23°C)
333	Pyrophoric liquid
X333	Pyrophoric liquid which reacts dangerously with water
336	Highly flammable liquid, toxic
338	Highly flammable liquid, corrosive
X338	Highly flammable liquid, corrosive, which reacts dangerously with water
339	Highly flammable liquid which can spontaneously lead to violent reaction
36	Flammable liquid (flash-point between 23°C and 60°C, inclusive), slightly toxic, or self-heating liquid, toxic
362	Flammable liquid, toxic, which reacts with water, emitting flammable gas
X362	Flammable liquid, toxic, which reacts dangerously with water, emitting flammable gases
368	Flammable liquid, toxic, corrosive
38	Flammable liquid (flash-point between 23°C and 60°C, inclusive), slightly corrosive or self-heating liquid, corrosive
382	Flammable liquid, corrosive, which reacts with water, emitting flammable gases
X382	Flammable liquid, corrosive, which reacts dangerously with water, emitting flammable gases
39	Flammable liquid, which can spontaneously lead to violent reaction
40	Flammable solid, or self-reactive substance, or self-heating substance, or polymerizing substance

HAZARD IDENTIFICATION NUMBERS
DISPLAYED ON SOME INTERMODAL CONTAINERS

423	Solid which reacts with water, emitting flammable gases, or flammable solid which reacts with water, emitting flammable gases, or self-heating solid which reacts with water, emitting flammable gases
X423	Solid which reacts dangerously with water, emitting flammable gases, or flammable solid which reacts dangerously with water, emitting flammable gases, or self-heating solid which reacts dangerously with water, emitting flammable gases
43	Spontaneously flammable (pyrophoric) solid
X432	Spontaneously flammable (pyrophoric) solid which reacts dangerously with water, emitting flammable gases
44	Flammable solid, in the molten state at an elevated temperature
446	Flammable solid, toxic, in the molten state at an elevated temperature
46	Flammable or self-heating solid, toxic
462	Toxic solid which reacts with water, emitting flammable gases
X462	Solid which reacts dangerously with water, emitting toxic gases
48	Flammable or self-heating solid, corrosive
482	Corrosive solid which reacts with water, emitting flammable gases
X482	Solid which reacts dangerously with water, emitting corrosive gases
50	Oxidizing (fire-intensifying) substance
539	Flammable organic peroxide
55	Strongly oxidizing (fire-intensifying) substance
556	Strongly oxidizing (fire-intensifying) substance, toxic
558	Strongly oxidizing (fire-intensifying) substance, corrosive
559	Strongly oxidizing (fire-intensifying) substance which can spontaneously lead to violent reaction
56	Oxidizing substance (fire-intensifying), toxic
568	Oxidizing substance (fire-intensifying), toxic, corrosive
58	Oxidizing substance (fire-intensifying), corrosive
59	Oxidizing substance (fire-intensifying), which can spontaneously lead to violent reaction
60	Toxic or slightly toxic substance
606	Infectious substance
623	Toxic liquid, which reacts with water, emitting flammable gases
63	Toxic substance, flammable (flash-point between 23°C and 60°C, inclusive)
638	Toxic substance, flammable, (flash-point between 23°C and 60°C, inclusive), corrosive
639	Toxic substance, flammable, (flash-point not above 60°C) which can spontaneously lead to violent reaction
64	Toxic solid, flammable or self-heating
642	Toxic solid which reacts with water, emitting flammable gases
65	Toxic substance, oxidizing (fire-intensifying)
66	Highly toxic substance

HAZARD IDENTIFICATION NUMBERS
DISPLAYED ON SOME INTERMODAL CONTAINERS

663	Highly toxic substance, flammable (flash-point not above 60°C)
664	Highly toxic solid, flammable or self-heating
665	Highly toxic substance, oxidizing (fire-intensifying)
668	Highly toxic substance, corrosive
X668	Highly toxic substance, corrosive, which reacts dangerously with water
669	Highly toxic substance which can spontaneously lead to violent reaction
68	Toxic substance, corrosive
69	Toxic or slightly toxic substance which can spontaneously lead to violent reaction
70	Radioactive material
768	Radioactive material, toxic, corrosive
78	Radioactive material, corrosive
80	Corrosive or slightly corrosive substance
X80	Corrosive or slightly corrosive substance which reacts dangerously with water
823	Corrosive liquid which reacts with water, emitting flammable gases
83	Corrosive or slightly corrosive substance, flammable (flash-point between 23°C and 60°C, inclusive)
X83	Corrosive or slightly corrosive substance, flammable (flash-point between 23°C and 60°C, inclusive), which reacts dangerously with water
839	Corrosive or slightly corrosive substance, flammable (flash-point between 23°C and 60°C, inclusive), which can spontaneously lead to violent reaction
X839	Corrosive or slightly corrosive substance, flammable (flash-point between 23°C and 60°C, inclusive), which can spontaneously lead to violent reaction and which reacts dangerously with water
84	Corrosive solid, flammable or self-heating
842	Corrosive solid which reacts with water, emitting flammable gases
85	Corrosive or slightly corrosive substance, oxidizing (fire-intensifying)
856	Corrosive or slightly corrosive substance, oxidizing (fire-intensifying) and toxic
86	Corrosive or slightly corrosive substance, toxic
88	Highly corrosive substance
X88	Highly corrosive substance which reacts dangerously with water
883	Highly corrosive substance, flammable (flash-point between 23°C and 60°C, inclusive)
884	Highly corrosive solid, flammable or self-heating
885	Highly corrosive substance, oxidizing (fire-intensifying)
886	Highly corrosive substance, toxic
X886	Highly corrosive substance, toxic, which reacts dangerously with water
89	Corrosive or slightly corrosive substance which can spontaneously lead to violent reaction
90	Environmentally hazardous substance; miscellaneous dangerous substances
99	Miscellaneous dangerous substance carried at an elevated temperature

PIPELINE TRANSPORTATION

In North America, hazardous materials/dangerous goods are commonly transported through millions of miles of pipelines and related structures. Products transported include natural gas, natural gas liquids, crude oil, gasoline, diesel fuel, anhydrous ammonia, carbon dioxide, jet fuel, and other commodities. Although most pipelines are buried, often there are aboveground structures and markers indicating the presence of pipelines. First responders should be aware of the pipelines in their jurisdictions, the products they transport, and the operators responsible for those pipelines. Proactive relationships can be beneficial in the safe and effective management of pipeline emergencies.

Types of Pipelines

Natural Gas Pipelines

Natural Gas Transmission Pipelines

Large-diameter, steel pipelines transport flammable natural gas (toxic and non-toxic) at very high pressures ranging from 200 to 1,500 psi*. Natural gas in transmission pipelines is odorless — generally *not odorized* with mercaptan (the "rotten egg" smell); however, natural gas containing hydrogen sulfide (H_2S) will have a distinct "rotten egg" odor.

Natural Gas Distribution Pipelines

Natural gas is delivered directly to customers via distribution pipelines. These pipelines are typically smaller-diameter, lower-pressure pipelines constructed of steel, plastic, or cast iron. Natural gas in distribution pipelines *is odorized* with mercaptan (the "rotten egg" smell).

Natural Gas-Gathering and Natural Gas Well Production Pipelines

Natural gas-gathering/well production pipelines collect "raw" natural gas from wellheads and transport the product to gas-processing and/or gas-treating plants. These gathering pipelines carry natural gas mixed with some quantity of natural gas liquids, water, and, in some areas, contaminants such as toxic hydrogen sulfide (H_2S). Natural gas in these pipelines is *not odorized* with mercaptan (the "rotten egg" smell); however, natural gas that contains hydrogen sulfide (H_2S) will have a distinct "rotten egg" odor.

Hazardous Liquid and Highly Volatile Liquid Pipelines

Hazardous Liquid Pipelines

Crude oil, refined petroleum products (e.g. gasoline, kerosene, jet fuel or diesel) and hazardous liquids (e.g. anhydrous ammonia or ethanol) are often transported by pipelines.

Many liquid petroleum pipelines transport different types of liquid petroleum in the same pipeline. To do so, the pipeline operator sends different products in "batches." For example, an operator could send gasoline for several hours, and then switch to jet fuels, before switching to diesel fuel.

* Data from http://naturalgas.org/naturalgas/transport/

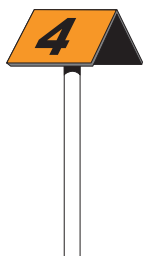
Highly Volatile Liquid (HVL) Pipelines

HVL pipelines transport hazardous liquids which will form a vapor cloud when released to the atmosphere and which have a vapor pressure exceeding 276 KPa (40 psia) at 37.8°C (100°F). An example of an HVL is liquid propane.

Pipeline Markers

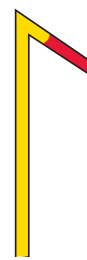
Since pipelines are usually buried underground, pipeline markers are used to indicate their presence in an area along the pipeline route. Of the three types of pipelines typically buried underground — distribution, gathering, and transmission — only transmission pipelines are marked with the following above-ground markers used to indicate their route.













Markers warn that a transmission pipeline is located in the area, identify the product transported in the line, and provide the name and telephone number of the pipeline operator to call. Markers and warning signs are located at frequent intervals along natural gas and liquid transmission pipeline rights-of-way, and are located at prominent points such as where pipelines intersect streets, highways, railways, or waterways.

Pipeline markers only indicate the presence of a pipeline—they do not indicate the exact location of the pipeline. Pipeline locations within a right-of-way may vary along its length and there may be multiple pipelines located in the same right-of-way.

NOTE:

- Markers for pipelines transporting materials containing dangerous levels of hydrogen sulfide (H_2S) may have markers that say: “Sour” or “Poison.”
- Natural gas distribution pipelines are not marked with above-ground signs.
- Gathering/production pipelines are often not marked with above-ground signs.

Pipeline Structures (Above Ground)

Natural Gas Transmission Pipelines:	Compressor stations, valves, metering stations.
Natural Gas Distribution Pipelines:	Regulator stations, customer meters and regulators, valve box covers.
Natural Gas Gathering/Well Production Pipelines:	Compressor stations, valves, metering stations, wellheads, piping, manifolds.
Petroleum and Hazardous Liquids Pipelines:	Storage tanks, valves, pump stations, loading racks.

Indications of Pipeline Leaks and Ruptures

Pipeline releases can range from relatively minor leaks to catastrophic ruptures. It is important to remember that gases and liquids behave differently once they are released from a pipeline. Generally, the following could be indications of a pipeline leak or rupture:

- Hissing, roaring, or explosive sound
- Flames appearing from the ground or water (perhaps very large flames)
- Vapor cloud/fog/mist
- Dirt/debris/water blowing out of the ground
- Liquids bubbling up from the ground or bubbling in water
- Distinctive, unusually strong odor of rotten eggs, mercaptan (an odorant in some natural gas pipelines), skunk, or petroleum
- Discolored/dead vegetation or discolored snow above a pipeline right-of-way
- Oil slick or sheen on flowing/standing water
- An area of frozen ground in the summer
- An unusual area of melted snow in the winter

General Considerations for Responding to a Pipeline Emergency

- **Safety First!** Your safety and the safety of the community you protect is top priority. Remember to approach a pipeline incident from upwind, uphill, and upstream while using air monitoring equipment to detect for the presence of explosive and/or toxic levels of hazardous materials/dangerous goods.
  - Always wear proper personal protective equipment. Be prepared for a flash fire. Use shielding to protect first responders in the event of an explosion. Use respiratory protection.
  - Never operate pipeline valves (except in coordination with the pipeline operator); this could make the incident worse and put you and others in danger.
  - Never attempt to extinguish a pipeline fire before supply is shut off; this could result in the accumulation of a large flammable/explosive vapor cloud or liquid pool that could make the incident worse and put you and others in danger.
  - Do not walk or drive into a vapor cloud in an attempt to identify the product(s) involved.
  - Do not park over manholes or storm drains.
  - Do not approach the scene with vehicles or mechanical equipment until the isolation zones have been established (vehicles are a potential ignition source).
- **Secure the site** and determine a plan to evacuate or shelter-in-place. Work with other responders to deny entry to an area.
- **Identify the product and the operator**. If safe to do so, you may be able to identify the product based on its characteristics or other external clues. Look for pipeline markers indicating the product, operator of the pipeline, and their emergency contact information. Pipelines transport many different types of products, including gases, liquids, and highly volatile liquids that are in a liquid state inside the pipeline but in a gaseous state if released from the pipeline. The vapor density of gases determines if they rise or sink in air. Viscosity and specific gravity also are important characteristics of hazardous liquids to consider. Identification of the product also will help you determine the appropriate distance for isolation of the affected area.
- **Notify the pipeline operator** using the emergency contact information on the pipeline marker or other contact information you may have received from the pipeline operator. The pipeline operator will be a resource to you in the response.
- **Establish a command post**. Implement the Incident Command Structure, as needed, and be prepared to implement a Unified Command as additional stakeholders and resources arrive.

Other Important Considerations

- If no flames are present, do not introduce ignition sources such as open flames, running vehicles, or electrical equipment (cell phones, pagers, two-way radios, lights, garage door openers, fans, door bells, etc.).
- Abandon any equipment used in or near the area of the pipeline release.
- If there is no risk to your safety or the safety of others, move far enough away from any noise coming from the pipeline to allow for normal conversation.
- Pipelines often are close to other public utilities, railroads, and highways; these can be impacted by pipeline releases or may be potential ignition sources.
- Natural gas can migrate underground from the source of a release to other areas via the path of least resistance (including through sewers, water lines, and geologic formations).

Considerations for Establishing Protective Action Distances

- Type of product
  - If you know the material involved, identify the three-digit guide number by looking up the name in the alphabetical list (blue-bordered pages), then using the three-digit guide number, consult the recommendations in the assigned guide.
- Pressure and diameter of pipe (the pipeline operator can tell you this if you don't already know it)
- Timing of valve closure by the pipeline operator (quickly for automated valves; longer for manually operated valves)
- Dissipation time of the product in the pipeline once valves are closed
- Ability to conduct atmospheric monitoring and/or air sampling
- Weather (wind direction, etc.)
- Local variables such as topography, population density, demographics, and fire suppression methods available
- Nearby building construction material/density
- Natural and man-made barriers (such as highways, railroads, rivers, etc.)

U.S. Pipeline Resources

U.S. Pipeline Locations: The National Pipeline Mapping System (NPMS) *https://www.npms.phmsa.dot.gov* indicates the general locations of hazardous liquids and natural gas transmission pipelines found within the U.S. The pipelines depicted in the NPMS are within 500 feet of their actual locations. Emergency responders may apply for an NPMS web viewer account that will allow access to more detailed information than is available to the general public. The NPMS does not contain gathering/production or natural gas distribution pipelines.

U.S. Pipeline Emergency Response Training: Where appropriate, reference pipeline emergencies training materials produced by the Pipeline and Hazardous Materials Safety Administration. Your state or jurisdiction also may provide training on how to handle the response to a pipeline incident.

Other Resources:

Pipeline Association for Public Awareness
https://www.pipelineawareness.org/

U.S. DOT, Pipeline and Hazardous Materials Safety Administration
https://www.phmsa.dot.gov/safety-awareness/pipeline/safety-awareness-overview

Pipeline Emergency Responders Initiative (PERI)
https://www.phmsa.dot.gov/pipeline/peri/pipeline-emergency-responders-initiative-peri

Canadian Pipeline Resources

Canadian Pipeline Locations: The Canadian Energy Pipeline Association (CEPA) provides the general locations of natural gas and liquid pipelines found within Canada.

https://www.cepa.com

INTRODUCTION TO YELLOW PAGES

For entries highlighted in green follow these steps:

- **IF THERE IS NO FIRE**:
  - Go directly to **Table 1** (green-bordered pages)
  - Look up the ID number and name of material
  - Identify initial isolation and protective action distances
  - Also consult the appropriate Orange Guide

- **IF A FIRE IS INVOLVED**:
  - Use the appropriate Orange Guide for **EVACUATION** distances
  - Also protect in downwind direction according to Table 1 for residual material release

Note 1: If the name in **Table 1** is shown with **(when spilled in water)**, these materials produce large amounts of Toxic Inhalation Hazard (TIH) (PIH in the US) gases when spilled in water. Some Water Reactive materials are also TIH materials themselves (e.g., UN1746 (Bromine trifluoride), UN1836 (Thionyl chloride)). In these instances, two entries are provided in **Table 1** for land-based and water-based spills. If a water-reactive material only has one entry in Table 1 for **(when spilled in water)** and the product is NOT spilled in water, Table 1 and Table 2 do not apply. You will find safe distances in the appropriate orange-bordered guide.

Note 2: **Explosives** are not individually listed by their ID number because in an emergency situation, the response will be based only on the division of the explosive, not on the individual explosive.

For divisions 1.1, 1.2, 1.3 and 1.5, refer to GUIDE 112.

For divisions 1.4 and 1.6, refer to GUIDE 114.

Note 3: Chemical warfare agents do not have an assigned ID number because they are not commercially transported. In an emergency situation, the assigned orange guide will provide guidance for the initial response. Also consult “Criminal or Terrorist Use of Chemical, Biological and Radiological Agents”, pp. 368 to 372.

ID No.	Guide No.	Name of Material
——	117	AC
——	154	Adamsite
——	112	Ammonium nitrate-fuel oil mixtures
——	158	Biological agents
——	112	Blasting agent, n.o.s.
——	153	Buzz
——	153	BZ
——	159	CA
——	125	CG
——	125	CK
——	153	CN
——	153	CS
——	154	CX
——	151	DA
——	153	DC
——	154	DM
——	125	DP
——	151	ED
——	112	Explosives, division 1.1, 1.2, 1.3 or 1.5
——	114	Explosives, division 1.4 or 1.6
——	153	GA
——	153	GB
——	153	GD
——	153	GF
——	153	H
——	153	HD
——	153	HL
——	153	HN-1
——	153	HN-2
——	153	HN-3
——	153	L (Lewisite)
——	153	Lewisite
——	152	MD
——	153	Mustard
——	153	Mustard Lewisite
——	152	PD
——	119	SA
——	153	Sarin
——	153	Soman
——	153	Tabun
——	153	Thickened GD
——	153	Toxins
——	153	VX
1001	116	Acetylene, dissolved
1002	122	Air, compressed
1003	122	Air, refrigerated liquid (cryogenic liquid)
1005	125	Ammonia, anhydrous
1005	125	Anhydrous ammonia
1006	120	Argon
1006	120	Argon, compressed
1008	125	Boron trifluoride
1008	125	Boron trifluoride, compressed
1009	126	Bromotrifluoromethane
1009	126	Refrigerant gas R-13B1
1010	116P	Butadienes, stabilized
1010	116P	Butadienes and hydrocarbon mixture, stabilized
1010	116P	Hydrocarbon and butadienes mixture, stabilized
1011	115	Butane
1012	115	Butylene

ID No.	Guide No.	Name of Material
1013	120	Carbon dioxide
1013	120	Carbon dioxide, compressed
1014	122	Carbon dioxide and Oxygen mixture, compressed
1014	122	Oxygen and Carbon dioxide mixture, compressed
1015	126	Carbon dioxide and Nitrous oxide mixture
1015	126	Nitrous oxide and Carbon dioxide mixture
1016	119	Carbon monoxide
1016	119	Carbon monoxide, compressed
1017	124	Chlorine
1018	126	Chlorodifluoromethane
1018	126	Refrigerant gas R-22
1020	126	Chloropentafluoroethane
1020	126	Refrigerant gas R-115
1021	126	1-Chloro-1,2,2,2-tetrafluoroethane
1021	126	Refrigerant gas R-124
1022	126	Chlorotrifluoromethane
1022	126	Refrigerant gas R-13
1023	119	Coal gas
1023	119	Coal gas, compressed
1026	119	Cyanogen
1027	115	Cyclopropane
1028	126	Dichlorodifluoromethane
1028	126	Refrigerant gas R-12
1029	126	Dichlorofluoromethane
1029	126	Refrigerant gas R-21
1030	115	1,1-Difluoroethane
1030	115	Refrigerant gas R-152a
1032	118	Dimethylamine, anhydrous
1033	115	Dimethyl ether
1035	115	Ethane
1035	115	Ethane, compressed
1036	118	Ethylamine
1037	115	Ethyl chloride
1038	115	Ethylene, refrigerated liquid (cryogenic liquid)
1039	115	Ethyl methyl ether
1039	115	Methyl ethyl ether
1040	119P	Ethylene oxide
1040	119P	Ethylene oxide with Nitrogen
1041	115	Carbon dioxide and Ethylene oxide mixture, with more than 9% but not more than 87% Ethylene oxide
1041	115	Ethylene oxide and Carbon dioxide mixture, with more than 9% but not more than 87% Ethylene oxide
1043	125	Fertilizer, ammoniating solution, with free Ammonia
1044	126	Fire extinguishers with compressed or liquefied gas
1045	124	Fluorine
1045	124	Fluorine, compressed
1046	120	Helium
1046	120	Helium, compressed
1048	125	Hydrogen bromide, anhydrous
1049	115	Hydrogen
1049	115	Hydrogen, compressed
1050	125	Hydrogen chloride, anhydrous
1051	117P	Hydrogen cyanide, anhydrous, stabilized
1051	117P	Hydrogen cyanide, stabilized
1052	125	Hydrogen fluoride, anhydrous

ID No.	Guide No.	Name of Material
1053	117	Hydrogen sulfide
1053	117	Hydrogen sulphide
1055	115	Isobutylene
1056	120	Krypton
1056	120	Krypton, compressed
1057	115	Lighter refills containing flammable gas
1057	115	Lighters containing flammable gas
1057	128	Lighters, non-pressurized, containing flammable liquid
1058	120	Liquefied gases, non-flammable, charged with Nitrogen, Carbon dioxide or Air
1060	116P	Methylacetylene and Propadiene mixture, stabilized
1060	116P	Propadiene and Methylacetylene mixture, stabilized
1061	118	Methylamine, anhydrous
1062	123	Methyl bromide
1063	115	Methyl chloride
1063	115	Refrigerant gas R-40
1064	117	Methyl mercaptan
1065	120	Neon
1065	120	Neon, compressed
1066	120	Nitrogen
1066	120	Nitrogen, compressed
1067	124	Dinitrogen tetroxide
1067	124	Nitrogen dioxide
1069	125	Nitrosyl chloride
1070	122	Nitrous oxide
1070	122	Nitrous oxide, compressed
1071	119	Oil gas
1071	119	Oil gas, compressed
1072	122	Oxygen
1072	122	Oxygen, compressed
1073	122	Oxygen, refrigerated liquid (cryogenic liquid)
1075	115	Butane
1075	115	Butylene
1075	115	Isobutane
1075	115	Isobutylene
1075	115	Liquefied petroleum gas
1075	115	LPG
1075	115	Petroleum gases, liquefied
1075	115	Propane
1075	115	Propylene
1076	125	Phosgene
1077	115	Propylene
1078	126	Dispersant gas, n.o.s.
1078	126	Refrigerant gas, n.o.s.
1079	125	Sulfur dioxide
1079	125	Sulphur dioxide
1080	126	Sulfur hexafluoride
1080	126	Sulphur hexafluoride
1081	116P	Tetrafluoroethylene, stabilized
1082	119P	Refrigerant gas R-1113
1082	119P	Trifluorochloroethylene, stabilized
1083	118	Trimethylamine, anhydrous
1085	116P	Vinyl bromide, stabilized
1086	116P	Vinyl chloride, stabilized
1087	116P	Vinyl methyl ether, stabilized
1088	127	Acetal

ID No.	Guide No.	Name of Material
1089	**129P**	Acetaldehyde
1090	**127**	Acetone
1091	**127**	Acetone oils
1092	**131P**	Acrolein, stabilized
1093	**131P**	Acrylonitrile, stabilized
1098	**131**	Allyl alcohol
1099	**131P**	Allyl bromide
1100	**131P**	Allyl chloride
1104	**129**	Amyl acetates
1105	**129**	Pentanols
1106	**132**	Amylamine
1107	**129**	Amyl chloride
1108	**128**	n-Amylene
1108	**128**	1-Pentene
1109	**129**	Amyl formates
1110	**127**	n-Amyl methyl ketone
1110	**127**	Methyl amyl ketone
1111	**130**	Amyl mercaptan
1112	**128**	Amyl nitrate
1113	**129**	Amyl nitrite
1114	**130**	Benzene
1120	**129**	Butanols
1123	**129**	Butyl acetates
1125	**132**	n-Butylamine
1126	**130**	1-Bromobutane
1126	**130**	n-Butyl bromide
1127	**130**	n-Butyl chloride
1127	**130**	Chlorobutanes
1128	**129**	n-Butyl formate
1129	**129P**	Butyraldehyde
1130	**128**	Camphor oil
1131	**131**	Carbon bisulfide
1131	**131**	Carbon bisulphide
1131	**131**	Carbon disulfide
1131	**131**	Carbon disulphide
1133	**128**	Adhesives (flammable)
1134	**130**	Chlorobenzene
1135	**131**	Ethylene chlorohydrin
1136	**128**	Coal tar distillates, flammable
1139	**127**	Coating solution
1143	**131P**	Crotonaldehyde
1143	**131P**	Crotonaldehyde, stabilized
1144	**128**	Crotonylene
1145	**128**	Cyclohexane
1146	**128**	Cyclopentane
1147	**130**	Decahydronaphthalene
1148	**129**	Diacetone alcohol
1149	**128**	Butyl ethers
1149	**128**	Dibutyl ethers
1150	**130P**	1,2-Dichloroethylene
1152	**130**	Dichloropentanes
1153	**127**	Ethylene glycol diethyl ether
1154	**132**	Diethylamine
1155	**127**	Diethyl ether
1155	**127**	Ethyl ether
1156	**127**	Diethyl ketone
1157	**128**	Diisobutyl ketone
1158	**132**	Diisopropylamine
1159	**127**	Diisopropyl ether
1160	**132**	Dimethylamine, aqueous solution
1160	**132**	Dimethylamine, solution
1161	**129**	Dimethyl carbonate

ID No.	Guide No.	Name of Material
1162	155	Dimethyldichlorosilane
1163	131	Dimethylhydrazine, unsymmetrical
1164	130	Dimethyl sulfide
1164	130	Dimethyl sulphide
1165	127	Dioxane
1166	127	Dioxolane
1167	128P	Divinyl ether, stabilized
1169	127	Extracts, aromatic, liquid
1170	127	Ethanol
1170	127	Ethanol, solution
1170	127	Ethyl alcohol
1170	127	Ethyl alcohol, solution
1171	127	Ethylene glycol monoethyl ether
1172	129	Ethylene glycol monoethyl ether acetate
1173	129	Ethyl acetate
1175	130	Ethylbenzene
1176	129	Ethyl borate
1177	130	2-Ethylbutyl acetate
1178	130	2-Ethylbutyraldehyde
1179	127	Ethyl butyl ether
1180	130	Ethyl butyrate
1181	155	Ethyl chloroacetate
1182	155	Ethyl chloroformate
1183	139	Ethyldichlorosilane
1184	131	Ethylene dichloride
1185	131P	Ethyleneimine, stabilized
1188	127	Ethylene glycol monomethyl ether
1189	129	Ethylene glycol monomethyl ether acetate
1190	129	Ethyl formate
1191	129	Ethylhexaldehydes
1191	129	Octyl aldehydes
1192	129	Ethyl lactate
1193	127	Ethyl methyl ketone
1193	127	Methyl ethyl ketone
1194	131	Ethyl nitrite, solution
1195	129	Ethyl propionate
1196	155	Ethyltrichlorosilane
1197	127	Extracts, flavoring, liquid
1197	127	Extracts, flavouring, liquid
1198	132	Formaldehyde, solution, flammable
1198	132	Formalin (flammable)
1199	153P	Furaldehydes
1201	127	Fusel oil
1202	128	Diesel fuel
1202	128	Fuel oil
1202	128	Gas oil
1202	128	Heating oil, light
1203	128	Gasohol
1203	128	Gasoline
1203	128	Motor spirit
1203	128	Petrol
1204	127	Nitroglycerin, solution in alcohol, with not more than 1% Nitroglycerin
1206	128	Heptanes
1207	130	Hexaldehyde
1208	128	Hexanes
1208	128	Neohexane
1210	129	Ink, printer's, flammable
1210	129	Printing ink, flammable

ID No.	Guide No.	Name of Material
1210	129	Printing ink related material, flammable
1212	129	Isobutanol
1212	129	Isobutyl alcohol
1213	129	Isobutyl acetate
1214	132	Isobutylamine
1216	128	Isooctenes
1218	130P	Isoprene, stabilized
1219	129	Isopropanol
1219	129	Isopropyl alcohol
1220	129	Isopropyl acetate
1221	132	Isopropylamine
1222	130	Isopropyl nitrate
1223	128	Kerosene
1224	127	Ketones, liquid, n.o.s.
1228	131	Mercaptan mixture, liquid, flammable, poisonous, n.o.s.
1228	131	Mercaptan mixture, liquid, flammable, toxic, n.o.s.
1228	131	Mercaptans, liquid, flammable, poisonous, n.o.s.
1228	131	Mercaptans, liquid, flammable, toxic, n.o.s.
1229	129	Mesityl oxide
1230	131	Methanol
1230	131	Methyl alcohol
1231	129	Methyl acetate
1233	130	Methylamyl acetate
1234	127	Methylal
1235	132	Methylamine, aqueous solution
1237	129	Methyl butyrate
1238	155	Methyl chloroformate
1239	131	Methyl chloromethyl ether
1242	139	Methyldichlorosilane
1243	129	Methyl formate
1244	131	Methylhydrazine
1245	127	Methyl isobutyl ketone
1246	127P	Methyl isopropenyl ketone, stabilized
1247	129P	Methyl methacrylate monomer, stabilized
1248	129	Methyl propionate
1249	127	Methyl propyl ketone
1250	155	Methyltrichlorosilane
1251	131P	Methyl vinyl ketone, stabilized
1259	131	Nickel carbonyl
1261	129	Nitromethane
1262	128	Isooctane
1262	128	Octanes
1263	128	Paint (flammable)
1263	128	Paint related material (flammable)
1264	129	Paraldehyde
1265	128	Isopentane
1265	128	Pentanes
1266	127	Perfumery products, with flammable solvents
1267	128	Petroleum crude oil
1268	128	Petroleum distillates, n.o.s.
1268	128	Petroleum products, n.o.s.
1270	128	Oil, petroleum
1270	128	Petroleum oil
1272	129	Pine oil
1274	129	n-Propanol
1274	129	Propyl alcohol, normal
1275	129P	Propionaldehyde

ID No.	Guide No.	Name of Material
1276	129	n-Propyl acetate
1277	132	Propylamine
1278	129	1-Chloropropane
1278	129	Propyl chloride
1279	130	1,2-Dichloropropane
1280	127P	Propylene oxide
1281	129	Propyl formates
1282	129	Pyridine
1286	127	Rosin oil
1287	127	Rubber solution
1288	128	Shale oil
1289	132	Sodium methylate, solution in alcohol
1292	129	Ethyl silicate
1292	129	Tetraethyl silicate
1293	127	Tinctures, medicinal
1294	130	Toluene
1295	139	Trichlorosilane
1296	132	Triethylamine
1297	132	Trimethylamine, aqueous solution
1298	155	Trimethylchlorosilane
1299	128	Turpentine
1300	128	Turpentine substitute
1301	129P	Vinyl acetate, stabilized
1302	127P	Vinyl ethyl ether, stabilized
1303	130P	Vinylidene chloride, stabilized
1304	127P	Vinyl isobutyl ether, stabilized
1305	155P	Vinyltrichlorosilane
1305	155P	Vinyltrichlorosilane, stabilized
1306	129	Wood preservatives, liquid
1307	130	Xylenes
1308	170	Zirconium suspended in a flammable liquid
1308	170	Zirconium suspended in a liquid (flammable)
1309	170	Aluminum powder, coated
1310	113	Ammonium picrate, wetted with not less than 10% water
1312	133	Borneol
1313	133	Calcium resinate
1314	133	Calcium resinate, fused
1318	133	Cobalt resinate, precipitated
1320	113	Dinitrophenol, wetted with not less than 15% water
1321	113	Dinitrophenolates, wetted with not less than 15% water
1322	113	Dinitroresorcinol, wetted with not less than 15% water
1323	170	Ferrocerium
1324	133	Films, nitrocellulose base
1325	133	Flammable solid, organic, n.o.s.
1325	133	Fusee (railway or highway)
1326	170	Hafnium powder, wetted with not less than 25% water
1327	133	Bhusa, wet, damp or contaminated with oil
1327	133	Hay, wet, damp or contaminated with oil
1327	133	Straw, wet, damp or contaminated with oil
1328	133	Hexamethylenetetramine
1330	133	Manganese resinate
1331	133	Matches, “strike anywhere”
1332	133	Metaldehyde
1333	170	Cerium, slabs, ingots or rods
1334	133	Naphthalene, crude

ID No.	Guide No.	Name of Material
1334	133	Naphthalene, refined
1336	113	Nitroguanidine, wetted with not less than 20% water
1336	113	Picrite, wetted with not less than 20% water
1337	113	Nitrostarch, wetted with not less than 20% water
1338	133	Phosphorus, amorphous
1338	133	Red phosphorus
1339	139	Phosphorus heptasulfide, free from yellow and white Phosphorus
1339	139	Phosphorus heptasulphide, free from yellow and white Phosphorus
1340	139	Phosphorus pentasulfide, free from yellow and white Phosphorus
1340	139	Phosphorus pentasulphide, free from yellow and white Phosphorus
1341	139	Phosphorus sesquisulfide, free from yellow and white Phosphorus
1341	139	Phosphorus sesquisulphide, free from yellow and white Phosphorus
1343	139	Phosphorus trisulfide, free from yellow and white Phosphorus
1343	139	Phosphorus trisulphide, free from yellow and white Phosphorus
1344	113	Picric acid, wetted with not less than 30% water
1344	113	Trinitrophenol, wetted with not less than 30% water
1345	133	Rubber scrap, powdered or granulated
1345	133	Rubber shoddy, powdered or granulated
1346	170	Silicon powder, amorphous
1347	113	Silver picrate, wetted with not less than 30% water
1348	113	Sodium dinitro-o-cresolate, wetted with not less than 15% water
1349	113	Sodium picramate, wetted with not less than 20% water
1350	133	Sulfur
1350	133	Sulphur
1352	170	Titanium powder, wetted with not less than 25% water
1353	133	Fabrics impregnated with weakly nitrated Nitrocellulose, n.o.s.
1353	133	Fibers impregnated with weakly nitrated Nitrocellulose, n.o.s.
1353	133	Fibres impregnated with weakly nitrated Nitrocellulose, n.o.s.
1354	113	Trinitrobenzene, wetted with not less than 30% water
1355	113	Trinitrobenzoic acid, wetted with not less than 30% water
1356	113	TNT, wetted with not less than 30% water
1356	113	Trinitrotoluene, wetted with not less than 30% water
1357	113	Urea nitrate, wetted with not less than 20% water
1358	170	Zirconium powder, wetted with not less than 25% water
1360	139	Calcium phosphide
1361	133	Carbon, animal or vegetable origin
1361	133	Charcoal
1362	133	Carbon, activated
1363	135	Copra
1364	133	Cotton waste, oily

ID No.	Guide No.	Name of Material
1365	133	Cotton
1365	133	Cotton, wet
1366	135	Diethylzinc
1369	135	p-Nitrosodimethylaniline
1370	135	Dimethylzinc
1372	133	Fibers, animal or vegetable, burnt, wet or damp
1372	133	Fibres, animal or vegetable, burnt, wet or damp
1373	133	Fabrics, animal or vegetable or synthetic, n.o.s. with oil
1373	133	Fibers, animal or vegetable or synthetic, n.o.s. with oil
1373	133	Fibres, animal or vegetable or synthetic, n.o.s. with oil
1374	133	Fish meal, unstabilized
1374	133	Fish scrap, unstabilized
1376	135	Iron oxide, spent
1376	135	Iron sponge, spent
1378	170	Metal catalyst, wetted
1379	133	Paper, unsaturated oil treated
1380	135	Pentaborane
1381	136	Phosphorus, white, dry or under water or in solution
1381	136	Phosphorus, yellow, dry or under water or in solution
1381	136	White phosphorus, dry or under water or in solution
1381	136	Yellow phosphorus, dry or under water or in solution
1382	135	Potassium sulfide, anhydrous
1382	135	Potassium sulfide, with less than 30% water of crystallization
1382	135	Potassium sulphide, anhydrous
1382	135	Potassium sulphide, with less than 30% water of crystallization
1383	135	Aluminum powder, pyrophoric
1383	135	Pyrophoric alloy, n.o.s.
1383	135	Pyrophoric metal, n.o.s.
1384	135	Sodium dithionite
1384	135	Sodium hydrosulfite
1384	135	Sodium hydrosulphite
1385	135	Sodium sulfide, anhydrous
1385	135	Sodium sulfide, with less than 30% water of crystallization
1385	135	Sodium sulphide, anhydrous
1385	135	Sodium sulphide, with less than 30% water of crystallization
1386	135	Seed cake, with more than 1.5% oil and not more than 11% moisture
1387	133	Wool waste, wet
1389	138	Alkali metal amalgam, liquid
1390	139	Alkali metal amides
1391	138	Alkali metal dispersion
1391	138	Alkaline earth metal dispersion
1392	138	Alkaline earth metal amalgam, liquid
1393	138	Alkaline earth metal alloy, n.o.s.
1394	138	Aluminum carbide
1395	139	Aluminum ferrosilicon powder
1396	138	Aluminum powder, uncoated
1397	139	Aluminum phosphide
1398	138	Aluminum silicon powder, uncoated
1400	138	Barium
1401	138	Calcium

ID No.	Guide No.	Name of Material
1402	138	Calcium carbide
1403	138	Calcium cyanamide, with more than 0.1% Calcium carbide
1404	138	Calcium hydride
1405	138	Calcium silicide
1407	138	Caesium
1407	138	Cesium
1408	139	Ferrosilicon
1409	138	Metal hydrides, water-reactive, n.o.s.
1410	138	Lithium aluminum hydride
1411	138	Lithium aluminum hydride, ethereal
1413	138	Lithium borohydride
1414	138	Lithium hydride
1415	138	Lithium
1417	138	Lithium silicon
1418	138	Magnesium alloys powder
1418	138	Magnesium powder
1419	139	Magnesium aluminum phosphide
1420	138	Potassium, metal alloys, liquid
1421	138	Alkali metal alloy, liquid, n.o.s.
1422	138	Potassium sodium alloys, liquid
1422	138	Sodium potassium alloys, liquid
1423	138	Rubidium
1426	138	Sodium borohydride
1427	138	Sodium hydride
1428	138	Sodium
1431	138	Sodium methylate, dry
1432	139	Sodium phosphide
1433	139	Stannic phosphides
1435	138	Zinc ashes
1435	138	Zinc dross
1435	138	Zinc residue
1435	138	Zinc skimmings
1436	138	Zinc dust
1436	138	Zinc powder
1437	138	Zirconium hydride
1438	140	Aluminum nitrate
1439	141	Ammonium dichromate
1442	143	Ammonium perchlorate
1444	140	Ammonium persulfate
1444	140	Ammonium persulphate
1445	141	Barium chlorate, solid
1446	141	Barium nitrate
1447	141	Barium perchlorate, solid
1448	141	Barium permanganate
1449	141	Barium peroxide
1450	140	Bromates, inorganic, n.o.s.
1451	140	Caesium nitrate
1451	140	Cesium nitrate
1452	140	Calcium chlorate
1453	140	Calcium chlorite
1454	140	Calcium nitrate
1455	140	Calcium perchlorate
1456	140	Calcium permanganate
1457	140	Calcium peroxide
1458	140	Borate and Chlorate mixture
1458	140	Chlorate and Borate mixture
1459	140	Chlorate and Magnesium chloride mixture, solid
1459	140	Magnesium chloride and Chlorate mixture, solid
1461	140	Chlorates, inorganic, n.o.s.

ID No.	Guide No.	Name of Material
1462	143	Chlorites, inorganic, n.o.s.
1463	141	Chromium trioxide, anhydrous
1465	140	Didymium nitrate
1466	140	Ferric nitrate
1467	143	Guanidine nitrate
1469	141	Lead nitrate
1470	141	Lead perchlorate, solid
1471	140	Lithium hypochlorite, dry
1471	140	Lithium hypochlorite mixture
1471	140	Lithium hypochlorite mixtures, dry
1472	143	Lithium peroxide
1473	140	Magnesium bromate
1474	140	Magnesium nitrate
1475	140	Magnesium perchlorate
1476	140	Magnesium peroxide
1477	140	Nitrates, inorganic, n.o.s.
1479	140	Oxidizing solid, n.o.s.
1481	140	Perchlorates, inorganic, n.o.s.
1482	140	Permanganates, inorganic, n.o.s.
1483	140	Peroxides, inorganic, n.o.s.
1484	140	Potassium bromate
1485	140	Potassium chlorate
1486	140	Potassium nitrate
1487	140	Potassium nitrate and Sodium nitrite mixture
1487	140	Sodium nitrite and Potassium nitrate mixture
1488	140	Potassium nitrite
1489	140	Potassium perchlorate
1490	140	Potassium permanganate
1491	144	Potassium peroxide
1492	140	Potassium persulfate
1492	140	Potassium persulphate
1493	140	Silver nitrate
1494	140	Sodium bromate
1495	140	Sodium chlorate
1496	143	Sodium chlorite
1498	140	Sodium nitrate
1499	140	Potassium nitrate and Sodium nitrate mixture
1499	140	Sodium nitrate and Potassium nitrate mixture
1500	141	Sodium nitrite
1502	140	Sodium perchlorate
1503	140	Sodium permanganate
1504	144	Sodium peroxide
1505	140	Sodium persulfate
1505	140	Sodium persulphate
1506	143	Strontium chlorate
1507	140	Strontium nitrate
1508	140	Strontium perchlorate
1509	143	Strontium peroxide
1510	143	Tetranitromethane
1511	140	Urea hydrogen peroxide
1512	140	Zinc ammonium nitrite
1513	140	Zinc chlorate
1514	140	Zinc nitrate
1515	140	Zinc permanganate
1516	143	Zinc peroxide
1517	113	Zirconium picramate, wetted with not less than 20% water
1541	155	Acetone cyanohydrin, stabilized
1544	151	Alkaloids, solid, n.o.s. (poisonous)

ID No.	Guide No.	Name of Material
1544	151	Alkaloid salts, solid, n.o.s. (poisonous)
1545	155	Allyl isothiocyanate, stabilized
1546	151	Ammonium arsenate
1547	153	Aniline
1548	153	Aniline hydrochloride
1549	157	Antimony compound, inorganic, solid, n.o.s.
1550	151	Antimony lactate
1551	151	Antimony potassium tartrate
1553	154	Arsenic acid, liquid
1554	154	Arsenic acid, solid
1555	151	Arsenic bromide
1556	152	Arsenic compound, liquid, n.o.s.
1556	152	Methyldichloroarsine
1557	152	Arsenic compound, solid, n.o.s.
1558	152	Arsenic
1559	151	Arsenic pentoxide
1560	157	Arsenic chloride
1560	157	Arsenic trichloride
1561	151	Arsenic trioxide
1562	152	Arsenical dust
1564	154	Barium compound, n.o.s.
1565	157	Barium cyanide
1566	154	Beryllium compound, n.o.s.
1567	134	Beryllium powder
1569	131	Bromoacetone
1570	152	Brucine
1571	113	Barium azide, wetted with not less than 50% water
1572	151	Cacodylic acid
1573	151	Calcium arsenate
1574	151	Calcium arsenate and Calcium arsenite mixture, solid
1574	151	Calcium arsenite and Calcium arsenate mixture, solid
1575	157	Calcium cyanide
1577	153	Chlorodinitrobenzenes, liquid
1578	152	Chloronitrobenzenes, solid
1579	153	4-Chloro-o-toluidine hydrochloride, solid
1580	154	Chloropicrin
1581	123	Chloropicrin and Methyl bromide mixture
1581	123	Methyl bromide and Chloropicrin mixture
1582	119	Chloropicrin and Methyl chloride mixture
1582	119	Methyl chloride and Chloropicrin mixture
1583	154	Chloropicrin mixture, n.o.s.
1585	151	Copper acetoarsenite
1586	151	Copper arsenite
1587	151	Copper cyanide
1588	157	Cyanides, inorganic, solid, n.o.s.
1589	125	Cyanogen chloride, stabilized
1590	153	Dichloroanilines, liquid
1591	152	o-Dichlorobenzene
1593	160	Dichloromethane
1593	160	Methylene chloride
1594	152	Diethyl sulfate
1594	152	Diethyl sulphate
1595	156	Dimethyl sulfate
1595	156	Dimethyl sulphate
1596	153	Dinitroanilines

ID No.	Guide No.	Name of Material
1597	152	Dinitrobenzenes, liquid
1598	153	Dinitro-o-cresol
1599	153	Dinitrophenol, solution
1600	152	Dinitrotoluenes, molten
1601	151	Disinfectant, solid, poisonous, n.o.s.
1601	151	Disinfectant, solid, toxic, n.o.s.
1602	151	Dye, liquid, poisonous, n.o.s.
1602	151	Dye, liquid, toxic, n.o.s.
1602	151	Dye intermediate, liquid, poisonous, n.o.s.
1602	151	Dye intermediate, liquid, toxic, n.o.s.
1603	155	Ethyl bromoacetate
1604	132	Ethylenediamine
1605	154	Ethylene dibromide
1606	151	Ferric arsenate
1607	151	Ferric arsenite
1608	151	Ferrous arsenate
1611	151	Hexaethyl tetraphosphate
1612	123	Compressed gas and hexaethyl tetraphosphate mixture
1612	123	Hexaethyl tetraphosphate and compressed gas mixture
1613	154	Hydrocyanic acid, aqueous solution, with less than 5% Hydrogen cyanide
1613	154	Hydrocyanic acid, aqueous solution, with not more than 20% Hydrogen cyanide
1613	154	Hydrogen cyanide, aqueous solution, with not more than 20% Hydrogen cyanide
1614	152	Hydrogen cyanide, stabilized (absorbed)
1616	151	Lead acetate
1617	151	Lead arsenates
1618	151	Lead arsenites
1620	151	Lead cyanide
1621	151	London purple
1622	151	Magnesium arsenate
1623	151	Mercuric arsenate
1624	154	Mercuric chloride
1625	141	Mercuric nitrate
1626	157	Mercuric potassium cyanide
1627	141	Mercurous nitrate
1629	151	Mercury acetate
1630	151	Mercury ammonium chloride
1631	154	Mercury benzoate
1634	154	Mercury bromides
1636	154	Mercury cyanide
1637	151	Mercury gluconate
1638	151	Mercury iodide
1639	151	Mercury nucleate
1640	151	Mercury oleate
1641	151	Mercury oxide
1642	151	Mercury oxycyanide, desensitized
1643	151	Mercury potassium iodide
1644	151	Mercury salicylate
1645	151	Mercury sulfate
1645	151	Mercury sulphate
1646	151	Mercury thiocyanate
1647	151	Ethylene dibromide and Methyl bromide mixture, liquid
1647	151	Methyl bromide and Ethylene dibromide mixture, liquid
1648	127	Acetonitrile

ID No.	Guide No.	Name of Material
1649	152	Motor fuel anti-knock mixture
1650	153	beta-Naphthylamine, solid
1650	153	Naphthylamine (beta), solid
1651	153	Naphthylthiourea
1652	153	Naphthylurea
1653	151	Nickel cyanide
1654	151	Nicotine
1655	151	Nicotine compound, solid, n.o.s.
1655	151	Nicotine preparation, solid, n.o.s.
1656	151	Nicotine hydrochloride, liquid
1656	151	Nicotine hydrochloride, solution
1657	151	Nicotine salicylate
1658	151	Nicotine sulfate, solution
1658	151	Nicotine sulphate, solution
1659	151	Nicotine tartrate
1660	124	Nitric oxide
1660	124	Nitric oxide, compressed
1661	153	Nitroanilines
1662	152	Nitrobenzene
1663	153	Nitrophenols
1664	152	Nitrotoluenes, liquid
1665	152	Nitroxylenes, liquid
1669	151	Pentachloroethane
1670	157	Perchloromethyl mercaptan
1671	153	Phenol, solid
1672	151	Phenylcarbylamine chloride
1673	153	Phenylenediamines
1674	151	Phenylmercuric acetate
1677	151	Potassium arsenate
1678	154	Potassium arsenite
1679	157	Potassium cuprocyanide
1680	157	Potassium cyanide, solid
1683	151	Silver arsenite
1684	151	Silver cyanide
1685	151	Sodium arsenate
1686	154	Sodium arsenite, aqueous solution
1687	153	Sodium azide
1688	152	Sodium cacodylate
1689	157	Sodium cyanide, solid
1690	154	Sodium fluoride, solid
1691	151	Strontium arsenite
1692	151	Strychnine
1692	151	Strychnine salts
1693	159	Tear gas devices
1693	159	Tear gas substance, liquid, n.o.s.
1694	159	Bromobenzyl cyanides, liquid
1695	131	Chloroacetone, stabilized
1697	153	Chloroacetophenone, solid
1698	154	Diphenylamine chloroarsine
1699	151	Diphenylchloroarsine, liquid
1700	159	Tear gas candles
1700	159	Tear gas grenades
1701	152	Xylyl bromide, liquid
1702	151	1,1,2,2-Tetrachloroethane
1704	153	Tetraethyl dithiopyrophosphate
1707	151	Thallium compound, n.o.s.
1708	153	Toluidines, liquid
1709	151	2,4-Toluenediamine, solid
1709	151	2,4-Toluylenediamine, solid
1710	160	Trichloroethylene
1711	153	Xylidines, liquid

ID No.	Guide No.	Name of Material
1712	151	Zinc arsenate
1712	151	Zinc arsenate and Zinc arsenite mixture
1712	151	Zinc arsenite
1712	151	Zinc arsenite and Zinc arsenate mixture
1713	151	Zinc cyanide
1714	139	Zinc phosphide
1715	137	Acetic anhydride
1716	156	Acetyl bromide
1717	155	Acetyl chloride
1718	153	Acid butyl phosphate
1718	153	Butyl acid phosphate
1719	154	Caustic alkali liquid, n.o.s.
1722	155	Allyl chlorocarbonate
1722	155	Allyl chloroformate
1723	132	Allyl iodide
1724	155	Allyltrichlorosilane, stabilized
1725	137	Aluminum bromide, anhydrous
1726	137	Aluminum chloride, anhydrous
1727	154	Ammonium bifluoride, solid
1727	154	Ammonium hydrogendifluoride, solid
1728	155	Amyltrichlorosilane
1729	156	Anisoyl chloride
1730	157	Antimony pentachloride, liquid
1731	157	Antimony pentachloride, solution
1732	157	Antimony pentafluoride
1733	157	Antimony trichloride
1733	157	Antimony trichloride, liquid
1733	157	Antimony trichloride, solid
1736	137	Benzoyl chloride
1737	156	Benzyl bromide
1738	156	Benzyl chloride
1739	137	Benzyl chloroformate
1740	154	Hydrogendifluorides, solid, n.o.s.
1741	125	Boron trichloride
1742	157	Boron trifluoride acetic acid complex, liquid
1743	157	Boron trifluoride propionic acid complex, liquid
1744	154	Bromine
1744	154	Bromine, solution
1744	154	Bromine, solution (Inhalation Hazard Zone A)
1744	154	Bromine, solution (Inhalation Hazard Zone B)
1745	144	Bromine pentafluoride
1746	144	Bromine trifluoride
1747	155	Butyltrichlorosilane
1748	140	Calcium hypochlorite, dry
1748	140	Calcium hypochlorite mixture, dry, with more than 39% available Chlorine (8.8% available Oxygen)
1749	124	Chlorine trifluoride
1750	153	Chloroacetic acid, solution
1751	153	Chloroacetic acid, solid
1752	156	Chloroacetyl chloride
1753	156	Chlorophenyltrichlorosilane
1754	137	Chlorosulfonic acid (with or without sulfur trioxide)
1754	137	Chlorosulphonic acid (with or without sulphur trioxide)
1755	154	Chromic acid, solution
1756	154	Chromic fluoride, solid

ID No.	Guide No.	Name of Material
1757	154	Chromic fluoride, solution
1758	137	Chromium oxychloride
1759	154	Corrosive solid, n.o.s.
1759	154	Ferrous chloride, solid
1760	154	Chemical kit
1760	154	Compounds, cleaning liquid (corrosive)
1760	154	Compounds, tree or weed killing, liquid (corrosive)
1760	154	Corrosive liquid, n.o.s.
1760	154	Ferrous chloride, solution
1761	154	Cupriethylenediamine, solution
1762	156	Cyclohexenyltrichlorosilane
1763	156	Cyclohexyltrichlorosilane
1764	153	Dichloroacetic acid
1765	156	Dichloroacetyl chloride
1766	156	Dichlorophenyltrichlorosilane
1767	155	Diethyldichlorosilane
1768	154	Difluorophosphoric acid, anhydrous
1769	156	Diphenyldichlorosilane
1770	153	Diphenylmethyl bromide
1771	156	Dodecyltrichlorosilane
1773	157	Ferric chloride, anhydrous
1774	154	Fire extinguisher charges, corrosive liquid
1775	154	Fluoroboric acid
1776	154	Fluorophosphoric acid, anhydrous
1777	137	Fluorosulfonic acid
1777	137	Fluorosulphonic acid
1778	154	Fluorosilicic acid
1778	154	Hydrofluorosilicic acid
1779	153	Formic acid
1779	153	Formic acid, with more than 85% acid
1780	156	Fumaryl chloride
1781	156	Hexadecyltrichlorosilane
1782	154	Hexafluorophosphoric acid
1783	153	Hexamethylenediamine, solution
1784	156	Hexyltrichlorosilane
1786	157	Hydrofluoric acid and Sulfuric acid mixture
1786	157	Hydrofluoric acid and Sulphuric acid mixture
1786	157	Sulfuric acid and Hydrofluoric acid mixture
1786	157	Sulphuric acid and Hydrofluoric acid mixture
1787	154	Hydriodic acid
1788	154	Hydrobromic acid
1789	157	Hydrochloric acid
1789	157	Muriatic acid
1790	157	Hydrofluoric acid
1791	154	Hypochlorite solution
1791	154	Sodium hypochlorite
1792	157	Iodine monochloride, solid
1793	153	Isopropyl acid phosphate
1794	154	Lead sulfate, with more than 3% free acid
1794	154	Lead sulphate, with more than 3% free acid
1796	157	Nitrating acid mixture with more than 50% nitric acid
1796	157	Nitrating acid mixture with not more than 50% nitric acid
1798	157	Aqua regia
1798	157	Nitrohydrochloric acid

ID No.	Guide No.	Name of Material
1799	156	Nonyltrichlorosilane
1800	156	Octadecyltrichlorosilane
1801	156	Octyltrichlorosilane
1802	157	Perchloric acid, with not more than 50% acid
1803	153	Phenolsulfonic acid, liquid
1803	153	Phenolsulphonic acid, liquid
1804	156	Phenyltrichlorosilane
1805	154	Phosphoric acid, solution
1806	137	Phosphorus pentachloride
1807	137	Phosphorus pentoxide
1808	137	Phosphorus tribromide
1809	137	Phosphorus trichloride
1810	137	Phosphorus oxychloride
1811	154	Potassium hydrogen difluoride, solid
1812	154	Potassium fluoride, solid
1813	154	Caustic potash, solid
1813	154	Potassium hydroxide, solid
1814	154	Caustic potash, solution
1814	154	Potassium hydroxide, solution
1815	132	Propionyl chloride
1816	155	Propyltrichlorosilane
1817	137	Pyrosulfuryl chloride
1817	137	Pyrosulphuryl chloride
1818	157	Silicon tetrachloride
1819	154	Sodium aluminate, solution
1823	154	Caustic soda, solid
1823	154	Sodium hydroxide, solid
1824	154	Caustic soda, solution
1824	154	Sodium hydroxide, solution
1825	157	Sodium monoxide
1826	157	Nitrating acid mixture, spent, with more than 50% nitric acid
1826	157	Nitrating acid mixture, spent, with not more than 50% nitric acid
1827	137	Stannic chloride, anhydrous
1827	137	Tin tetrachloride
1828	137	Sulfur chlorides
1828	137	Sulphur chlorides
1829	137	Sulfur trioxide, stabilized
1829	137	Sulphur trioxide, stabilized
1830	137	Sulfuric acid
1830	137	Sulfuric acid, with more than 51% acid
1830	137	Sulphuric acid
1830	137	Sulphuric acid, with more than 51% acid
1831	137	Sulfuric acid, fuming
1831	137	Sulphuric acid, fuming
1832	137	Sulfuric acid, spent
1832	137	Sulphuric acid, spent
1833	154	Sulfurous acid
1833	154	Sulphurous acid
1834	137	Sulfuryl chloride
1834	137	Sulphuryl chloride
1835	153	Tetramethylammonium hydroxide, solution
1836	137	Thionyl chloride
1837	157	Thiophosphoryl chloride
1838	137	Titanium tetrachloride
1839	153	Trichloroacetic acid
1840	154	Zinc chloride, solution
1841	171	Acetaldehyde ammonia

ID No.	Guide No.	Name of Material
1843	141	Ammonium dinitro-o-cresolate, solid
1845	120	Carbon dioxide, solid
1845	120	Dry ice
1846	151	Carbon tetrachloride
1847	153	Potassium sulfide, hydrated, with not less than 30% water of crystallization
1847	153	Potassium sulphide, hydrated, with not less than 30% water of crystallization
1848	153	Propionic acid
1848	153	Propionic acid, with not less than 10% and less than 90% acid
1849	153	Sodium sulfide, hydrated, with not less than 30% water
1849	153	Sodium sulphide, hydrated, with not less than 30% water
1851	151	Medicine, liquid, poisonous, n.o.s.
1851	151	Medicine, liquid, toxic, n.o.s.
1854	135	Barium alloys, pyrophoric
1855	135	Calcium, pyrophoric
1855	135	Calcium alloys, pyrophoric
1856	133	Rags, oily
1857	133	Textile waste, wet
1858	126	Hexafluoropropylene
1858	126	Hexafluoropropylene, compressed
1858	126	Refrigerant gas R-1216
1859	125	Silicon tetrafluoride
1859	125	Silicon tetrafluoride, compressed
1860	116P	Vinyl fluoride, stabilized
1862	130	Ethyl crotonate
1863	128	Fuel, aviation, turbine engine
1865	128	n-Propyl nitrate
1866	127	Resin solution
1868	134	Decaborane
1869	138	Magnesium
1869	138	Magnesium, in pellets, turnings or ribbons
1869	138	Magnesium alloys, with more than 50% Magnesium, in pellets, turnings or ribbons
1870	138	Potassium borohydride
1871	170	Titanium hydride
1872	140	Lead dioxide
1873	143	Perchloric acid, with more than 50% but not more than 72% acid
1884	157	Barium oxide
1885	153	Benzidine
1886	156	Benzylidene chloride
1887	160	Bromochloromethane
1888	151	Chloroform
1889	157	Cyanogen bromide
1891	131	Ethyl bromide
1892	151	Ethyldichloroarsine
1894	151	Phenylmercuric hydroxide
1895	151	Phenylmercuric nitrate
1897	160	Perchloroethylene
1897	160	Tetrachloroethylene
1898	156	Acetyl iodide
1902	153	Diisooctyl acid phosphate
1903	153	Disinfectant, liquid, corrosive, n.o.s.
1905	154	Selenic acid
1906	153	Acid, sludge

ID No.	Guide No.	Name of Material
1906	153	Sludge acid
1907	154	Soda lime, with more than 4% Sodium hydroxide
1908	154	Chlorite solution
1910	157	Calcium oxide
1911	119	Diborane
1911	119	Diborane, compressed
1911	119	Diborane mixtures
1912	115	Methyl chloride and Methylene chloride mixture
1912	115	Methylene chloride and Methyl chloride mixture
1913	120	Neon, refrigerated liquid (cryogenic liquid)
1914	130	Butyl propionates
1915	127	Cyclohexanone
1916	152	2,2'-Dichlorodiethyl ether
1916	152	Dichloroethyl ether
1917	129P	Ethyl acrylate, stabilized
1918	130	Cumene
1918	130	Isopropylbenzene
1919	129P	Methyl acrylate, stabilized
1920	128	Nonanes
1921	131P	Propyleneimine, stabilized
1922	132	Pyrrolidine
1923	135	Calcium dithionite
1923	135	Calcium hydrosulfite
1923	135	Calcium hydrosulphite
1928	138	Methyl magnesium bromide in Ethyl ether
1929	135	Potassium dithionite
1929	135	Potassium hydrosulfite
1929	135	Potassium hydrosulphite

ID No.	Guide No.	Name of Material
1931	171	Zinc dithionite
1931	171	Zinc hydrosulfite
1931	171	Zinc hydrosulphite
1932	135	Zirconium scrap
1935	157	Cyanide solution, n.o.s.
1938	156	Bromoacetic acid, solution
1939	137	Phosphorus oxybromide, solid
1940	153	Thioglycolic acid
1941	171	Dibromodifluoromethane
1941	171	Refrigerant gas R-12B2
1942	140	Ammonium nitrate, with not more than 0.2% combustible substances
1944	133	Matches, safety
1945	133	Matches, wax “vesta”
1950	126	Aerosols
1951	120	Argon, refrigerated liquid (cryogenic liquid)
1952	126	Carbon dioxide and Ethylene oxide mixtures, with not more than 9% Ethylene oxide
1952	126	Ethylene oxide and Carbon dioxide mixtures, with not more than 9% Ethylene oxide
1953	119	Compressed gas, poisonous, flammable, n.o.s.
1953	119	Compressed gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone A)
1953	119	Compressed gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone B)
1953	119	Compressed gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone C)
1953	119	Compressed gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone D)

ID No.	Guide No.	Name of Material
1953	119	Compressed gas, toxic, flammable, n.o.s.
1953	119	Compressed gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone A)
1953	119	Compressed gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone B)
1953	119	Compressed gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone C)
1953	119	Compressed gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone D)
1954	115	Compressed gas, flammable, n.o.s.
1954	115	Dispersant gases, n.o.s. (flammable)
1954	115	Refrigerant gases, n.o.s. (flammable)
1955	123	Compressed gas, poisonous, n.o.s.
1955	123	Compressed gas, poisonous, n.o.s. (Inhalation Hazard Zone A)
1955	123	Compressed gas, poisonous, n.o.s. (Inhalation Hazard Zone B)
1955	123	Compressed gas, poisonous, n.o.s. (Inhalation Hazard Zone C)
1955	123	Compressed gas, poisonous, n.o.s. (Inhalation Hazard Zone D)
1955	123	Compressed gas, toxic, n.o.s.
1955	123	Compressed gas, toxic, n.o.s. (Inhalation Hazard Zone A)
1955	123	Compressed gas, toxic, n.o.s. (Inhalation Hazard Zone B)
1955	123	Compressed gas, toxic, n.o.s. (Inhalation Hazard Zone C)
1955	123	Compressed gas, toxic, n.o.s. (Inhalation Hazard Zone D)
1955	123	Organic phosphate compound mixed with compressed gas
1955	123	Organic phosphate mixed with compressed gas
1955	123	Organic phosphorus compound mixed with compressed gas
1956	126	Compressed gas, n.o.s.
1957	115	Deuterium
1957	115	Deuterium, compressed
1958	126	1,2-Dichloro-1,1,2,2-tetrafluoroethane
1958	126	Refrigerant gas R-114
1959	116P	1,1-Difluoroethylene
1959	116P	Refrigerant gas R-1132a
1961	115	Ethane, refrigerated liquid
1961	115	Ethane-Propane mixture, refrigerated liquid
1961	115	Propane-Ethane mixture, refrigerated liquid
1962	116P	Ethylene
1962	116P	Ethylene, compressed
1963	120	Helium, refrigerated liquid (cryogenic liquid)
1964	115	Hydrocarbon gas mixture, compressed, n.o.s.
1965	115	Hydrocarbon gas mixture, liquefied, n.o.s.
1966	115	Hydrogen, refrigerated liquid (cryogenic liquid)
1967	123	Insecticide gas, poisonous, n.o.s.
1967	123	Insecticide gas, toxic, n.o.s.
1967	123	Parathion and compressed gas mixture

ID No.	Guide No.	Name of Material
1968	126	Insecticide gas, n.o.s.
1969	115	Isobutane
1970	120	Krypton, refrigerated liquid (cryogenic liquid)
1971	115	Methane
1971	115	Methane, compressed
1971	115	Natural gas, compressed
1972	115	Liquefied natural gas (cryogenic liquid)
1972	115	LNG (cryogenic liquid)
1972	115	Methane, refrigerated liquid (cryogenic liquid)
1972	115	Natural gas, refrigerated liquid (cryogenic liquid)
1973	126	Chlorodifluoromethane and Chloropentafluoroethane mixture
1973	126	Chloropentafluoroethane and Chlorodifluoromethane mixture
1973	126	Refrigerant gas R-502
1974	126	Chlorodifluorobromomethane
1974	126	Refrigerant gas R-12B1
1975	124	Dinitrogen tetroxide and Nitric oxide mixture
1975	124	Nitric oxide and Dinitrogen tetroxide mixture
1975	124	Nitric oxide and Nitrogen dioxide mixture
1975	124	Nitrogen dioxide and Nitric oxide mixture
1976	126	Octafluorocyclobutane
1976	126	Refrigerant gas RC-318
1977	120	Nitrogen, refrigerated liquid (cryogenic liquid)
1978	115	Propane
1982	126	Refrigerant gas R-14
1982	126	Refrigerant gas R-14, compressed
1982	126	Tetrafluoromethane
1982	126	Tetrafluoromethane, compressed
1983	126	1-Chloro-2,2,2-trifluoroethane
1983	126	Refrigerant gas R-133a
1984	126	Refrigerant gas R-23
1984	126	Trifluoromethane
1986	131	Alcohols, flammable, poisonous, n.o.s.
1986	131	Alcohols, flammable, toxic, n.o.s.
1987	127	Alcohols, n.o.s.
1987	127	Denatured alcohol
1988	131P	Aldehydes, flammable, poisonous, n.o.s.
1988	131P	Aldehydes, flammable, toxic, n.o.s.
1989	129P	Aldehydes, n.o.s.
1990	171	Benzaldehyde
1991	131P	Chloroprene, stabilized
1992	131	Flammable liquid, poisonous, n.o.s.
1992	131	Flammable liquid, toxic, n.o.s.
1993	128	Combustible liquid, n.o.s.
1993	128	Compounds, cleaning liquid (flammable)
1993	128	Compounds, tree or weed killing, liquid (flammable)
1993	128	Diesel fuel
1993	128	Flammable liquid, n.o.s.
1993	128	Fuel oil
1994	136	Iron pentacarbonyl

ID No.	Guide No.	Name of Material
1999	130	Asphalt
1999	130	Asphalt, cut back
1999	130	Tars, liquid
2000	133	Celluloid, in blocks, rods, rolls, sheets, tubes, etc., except scrap
2001	133	Cobalt naphthenates, powder
2002	135	Celluloid, scrap
2004	135	Magnesium diamide
2005	135	Magnesium diphenyl
2006	135	Plastics, nitrocellulose-based, self-heating, n.o.s.
2008	135	Zirconium powder, dry
2009	135	Zirconium, dry, finished sheets, strips or coiled wire
2010	138	Magnesium hydride
2011	139	Magnesium phosphide
2012	139	Potassium phosphide
2013	139	Strontium phosphide
2014	140	Hydrogen peroxide, aqueous solution, with not less than 20% but not more than 60% Hydrogen peroxide (stabilized as necessary)
2015	143	Hydrogen peroxide, aqueous solution, stabilized, with more than 60% Hydrogen peroxide
2015	143	Hydrogen peroxide, stabilized
2016	151	Ammunition, poisonous, non-explosive
2016	151	Ammunition, toxic, non-explosive
2017	159	Ammunition, tear-producing, non-explosive
2018	152	Chloroanilines, solid
2019	152	Chloroanilines, liquid
2020	153	Chlorophenols, solid
2021	153	Chlorophenols, liquid
2022	153	Cresylic acid
2023	131P	Epichlorohydrin
2024	151	Mercury compound, liquid, n.o.s.
2025	151	Mercury compound, solid, n.o.s.
2026	151	Phenylmercuric compound, n.o.s.
2027	151	Sodium arsenite, solid
2028	153	Bombs, smoke, non-explosive, with corrosive liquid, without initiating device
2029	132	Hydrazine, anhydrous
2030	153	Hydrazine, aqueous solution, with more than 37% Hydrazine
2031	157	Nitric acid, other than red fuming, with more than 65% nitric acid
2031	157	Nitric acid, other than red fuming, with not more than 65% nitric acid
2032	157	Nitric acid, red fuming
2033	154	Potassium monoxide
2034	115	Hydrogen and Methane mixture, compressed
2034	115	Methane and Hydrogen mixture, compressed
2035	115	Refrigerant gas R-143a
2035	115	1,1,1-Trifluoroethane
2036	120	Xenon
2036	120	Xenon, compressed
2037	115	Gas cartridges
2037	115	Receptacles, small, containing gas

ID No.	Guide No.	Name of Material
2038	152	Dinitrotoluenes, liquid
2044	115	2,2-Dimethylpropane
2045	130	Isobutyl aldehyde
2045	130	Isobutyraldehyde
2046	130	Cymenes
2047	129	Dichloropropenes
2048	130P	Dicyclopentadiene
2049	130	Diethylbenzene
2050	128	Diisobutylene, isomeric compounds
2051	132	2-Dimethylaminoethanol
2052	128	Dipentene
2053	129	Methylamyl alcohol
2053	129	Methyl isobutyl carbinol
2054	132	Morpholine
2055	128P	Styrene monomer, stabilized
2056	127	Tetrahydrofuran
2057	128	Tripropylene
2058	129	Valeraldehyde
2059	127	Nitrocellulose, solution, flammable
2067	140	Ammonium nitrate based fertilizer
2071	140	Ammonium nitrate based fertilizer
2073	125	Ammonia, solution, with more than 35% but not more than 50% Ammonia
2074	153P	Acrylamide, solid
2075	153	Chloral, anhydrous, stabilized
2076	153	Cresols, liquid
2077	153	alpha-Naphthylamine
2077	153	Naphthylamine (alpha)
2078	156	Toluene diisocyanate
2079	154	Diethylenetriamine
2186	125	Hydrogen chloride, refrigerated liquid
2187	120	Carbon dioxide, refrigerated liquid
2188	119	Arsine
2189	119	Dichlorosilane
2190	124	Oxygen difluoride
2190	124	Oxygen difluoride, compressed
2191	123	Sulfuryl fluoride
2191	123	Sulphuryl fluoride
2192	119	Germane
2193	126	Hexafluoroethane
2193	126	Hexafluoroethane, compressed
2193	126	Refrigerant gas R-116
2193	126	Refrigerant gas R-116, compressed
2194	125	Selenium hexafluoride
2195	125	Tellurium hexafluoride
2196	125	Tungsten hexafluoride
2197	125	Hydrogen iodide, anhydrous
2198	125	Phosphorus pentafluoride
2198	125	Phosphorus pentafluoride, compressed
2199	119	Phosphine
2200	116P	Propadiene, stabilized
2201	122	Nitrous oxide, refrigerated liquid
2202	117	Hydrogen selenide, anhydrous
2203	116	Silane
2203	116	Silane, compressed
2204	119	Carbonyl sulfide
2204	119	Carbonyl sulphide
2205	153	Adiponitrile

ID No.	Guide No.	Name of Material
2206	155	Isocyanate solution, poisonous, n.o.s.
2206	155	Isocyanate solution, toxic, n.o.s.
2206	155	Isocyanates, poisonous, n.o.s.
2206	155	Isocyanates, toxic, n.o.s.
2208	140	Bleaching powder
2208	140	Calcium hypochlorite mixture, dry, with more than 10% but not more than 39% available Chlorine
2209	153	Formaldehyde, solution (corrosive)
2209	153	Formalin (corrosive)
2210	135	Maneb
2210	135	Maneb preparation, with not less than 60% Maneb
2211	171	Polymeric beads, expandable
2212	171	Asbestos
2212	171	Asbestos, amphibole
2212	171	Asbestos, blue
2212	171	Asbestos, brown
2212	171	Blue asbestos
2212	171	Brown asbestos
2213	133	Paraformaldehyde
2214	156	Phthalic anhydride
2215	156	Maleic anhydride
2215	156	Maleic anhydride, molten
2216	171	Fish meal, stabilized
2216	171	Fish scrap, stabilized
2217	135	Seed cake, with not more than 1.5% oil and not more than 11% moisture
2218	132P	Acrylic acid, stabilized
2219	129	Allyl glycidyl ether
2222	128	Anisole
2224	152	Benzonitrile
2225	156	Benzenesulfonyl chloride
2225	156	Benzenesulphonyl chloride
2226	156	Benzotrichloride
2227	130P	n-Butyl methacrylate, stabilized
2232	153	Chloroacetaldehyde
2232	153	2-Chloroethanal
2233	152	Chloroanisidines
2234	130	Chlorobenzotrifluorides
2235	153	Chlorobenzyl chlorides, liquid
2236	156	3-Chloro-4-methylphenyl isocyanate, liquid
2237	153	Chloronitroanilines
2238	129	Chlorotoluenes
2239	153	Chlorotoluidines, solid
2240	154	Chromosulfuric acid
2240	154	Chromosulphuric acid
2241	128	Cycloheptane
2242	128	Cycloheptene
2243	130	Cyclohexyl acetate
2244	129	Cyclopentanol
2245	128	Cyclopentanone
2246	128	Cyclopentene
2247	128	n-Decane
2248	132	Di-n-butylamine
2249	131	Dichlorodimethyl ether, symmetrical
2250	156	Dichlorophenyl isocyanates
2251	128P	Bicyclo[2.2.1]hepta-2,5-diene, stabilized
2251	128P	2,5-Norbornadiene, stabilized

ID No.	Guide No.	Name of Material
2252	127	1,2-Dimethoxyethane
2253	153	N,N-Dimethylaniline
2254	133	Matches, fusee
2256	130	Cyclohexene
2257	138	Potassium
2258	132	1,2-Propylenediamine
2259	153	Triethylenetetramine
2260	132	Tripropylamine
2261	153	Xylenols, solid
2262	156	Dimethylcarbamoyl chloride
2263	128	Dimethylcyclohexanes
2264	132	N,N-Dimethylcyclohexylamine
2264	132	Dimethylcyclohexylamine
2265	129	N,N-Dimethylformamide
2266	132	Dimethyl-N-propylamine
2267	156	Dimethyl thiophosphoryl chloride
2269	153	3,3'-Iminodipropylamine
2270	132	Ethylamine, aqueous solution, with not less than 50% but not more than 70% Ethylamine
2271	128	Ethyl amyl ketone
2272	153	N-Ethylaniline
2273	153	2-Ethylaniline
2274	153	N-Ethyl-N-benzylaniline
2275	129	2-Ethylbutanol
2276	132	2-Ethylhexylamine
2277	130P	Ethyl methacrylate, stabilized
2278	128	n-Heptene
2279	151	Hexachlorobutadiene
2280	153	Hexamethylenediamine, solid
2281	156	Hexamethylene diisocyanate
2282	129	Hexanols
2283	130P	Isobutyl methacrylate, stabilized
2284	131	Isobutyronitrile
2285	156	Isocyanatobenzotrifluorides
2286	128	Pentamethylheptane
2287	128	Isoheptenes
2288	128	Isohexenes
2289	153	Isophoronediamine
2290	156	Isophorone diisocyanate
2291	151	Lead compound, soluble, n.o.s.
2293	128	4-Methoxy-4-methylpentan-2-one
2294	153	N-Methylaniline
2295	155	Methyl chloroacetate
2296	128	Methylcyclohexane
2297	128	Methylcyclohexanone
2298	128	Methylcyclopentane
2299	155	Methyl dichloroacetate
2300	153	2-Methyl-5-ethylpyridine
2301	128	2-Methylfuran
2302	127	5-Methylhexan-2-one
2303	128	Isopropenylbenzene
2304	133	Naphthalene, molten
2305	153	Nitrobenzenesulfonic acid
2305	153	Nitrobenzenesulphonic acid
2306	152	Nitrobenzotrifluorides, liquid
2307	152	3-Nitro-4-chlorobenzotrifluoride
2308	157	Nitrosylsulfuric acid, liquid
2308	157	Nitrosylsulphuric acid, liquid
2309	128P	Octadiene
2310	131	Pentane-2,4-dione
2311	153	Phenetidines

ID No.	Guide No.	Name of Material
2312	153	Phenol, molten
2313	129	Picolines
2315	171	Articles containing Polychlorinated biphenyls (PCB)
2315	171	PCB
2315	171	Polychlorinated biphenyls, liquid
2316	157	Sodium cuprocyanide, solid
2317	157	Sodium cuprocyanide, solution
2318	135	Sodium hydrosulfide, with less than 25% water of crystallization
2318	135	Sodium hydrosulphide, with less than 25% water of crystallization
2319	128	Terpene hydrocarbons, n.o.s.
2320	153	Tetraethylenepentamine
2321	153	Trichlorobenzenes, liquid
2322	152	Trichlorobutene
2323	130	Triethyl phosphite
2324	128	Triisobutylene
2325	129	1,3,5-Trimethylbenzene
2326	153	Trimethylcyclohexylamine
2327	153	Trimethylhexamethylenediamines
2328	156	Trimethylhexamethylene diisocyanate
2329	130	Trimethyl phosphite
2330	128	Undecane
2331	154	Zinc chloride, anhydrous
2332	129	Acetaldehyde oxime
2333	131	Allyl acetate
2334	131	Allylamine
2335	131	Allyl ethyl ether
2336	131	Allyl formate
2337	131	Phenyl mercaptan
2338	127	Benzotrifluoride
2339	130	2-Bromobutane
2340	130	2-Bromoethyl ethyl ether
2341	130	1-Bromo-3-methylbutane
2342	130	Bromomethylpropanes
2343	130	2-Bromopentane
2344	129	Bromopropanes
2345	130	3-Bromopropyne
2346	127	Butanedione
2346	127	Diacetyl
2347	130	Butyl mercaptan
2348	129P	Butyl acrylates, stabilized
2350	127	Butyl methyl ether
2351	129	Butyl nitrites
2352	127P	Butyl vinyl ether, stabilized
2353	132	Butyryl chloride
2354	131	Chloromethyl ethyl ether
2356	129	2-Chloropropane
2357	132	Cyclohexylamine
2358	128P	Cyclooctatetraene
2359	132	Diallylamine
2360	131P	Diallyl ether
2361	132	Diisobutylamine
2362	130	1,1-Dichloroethane
2363	129	Ethyl mercaptan
2364	128	n-Propyl benzene
2366	128	Diethyl carbonate
2367	130	alpha-Methylvaleraldehyde
2367	130	Methyl valeraldehyde (alpha)
2368	128	alpha-Pinene

ID No.	Guide No.	Name of Material
2368	128	Pinene (alpha)
2370	128	1-Hexene
2371	128	Isopentenes
2372	129	1,2-Di-(dimethylamino)ethane
2373	127	Diethoxymethane
2374	127	3,3-Diethoxypropene
2375	129	Diethyl sulfide
2375	129	Diethyl sulphide
2376	127	2,3-Dihydropyran
2377	127	1,1-Dimethoxyethane
2378	131	2-Dimethylaminoacetonitrile
2379	132	1,3-Dimethylbutylamine
2380	127	Dimethyldiethoxysilane
2381	131	Dimethyl disulfide
2381	131	Dimethyl disulphide
2382	131	Dimethylhydrazine, symmetrical
2383	132	Dipropylamine
2384	127	Di-n-propyl ether
2385	129	Ethyl isobutyrate
2386	132	1-Ethylpiperidine
2387	130	Fluorobenzene
2388	130	Fluorotoluenes
2389	128	Furan
2390	129	2-Iodobutane
2391	129	Iodomethylpropanes
2392	129	Iodopropanes
2393	129	Isobutyl formate
2394	129	Isobutyl propionate
2395	132	Isobutyryl chloride
2396	131P	Methacrylaldehyde, stabilized
2397	127	3-Methylbutan-2-one
2398	127	Methyl tert-butyl ether
2399	132	1-Methylpiperidine
2400	130	Methyl isovalerate
2401	132	Piperidine
2402	130	Propanethiols
2403	129P	Isopropenyl acetate
2404	131	Propionitrile
2405	129	Isopropyl butyrate
2406	127	Isopropyl isobutyrate
2407	155	Isopropyl chloroformate
2409	129	Isopropyl propionate
2410	129	1,2,3,6-Tetrahydropyridine
2411	131	Butyronitrile
2412	130	Tetrahydrothiophene
2413	128	Tetrapropyl orthotitanate
2414	130	Thiophene
2416	129	Trimethyl borate
2417	125	Carbonyl fluoride
2417	125	Carbonyl fluoride, compressed
2418	125	Sulfur tetrafluoride
2418	125	Sulphur tetrafluoride
2419	116	Bromotrifluoroethylene
2420	125	Hexafluoroacetone
2421	124	Nitrogen trioxide
2422	126	Octafluorobut-2-ene
2422	126	Refrigerant gas R-1318
2424	126	Octafluoropropane
2424	126	Refrigerant gas R-218
2426	140	Ammonium nitrate, liquid (hot concentrated solution)
2427	140	Potassium chlorate, aqueous solution

ID No.	Guide No.	Name of Material
2428	140	Sodium chlorate, aqueous solution
2429	140	Calcium chlorate, aqueous solution
2430	153	Alkylphenols, solid, n.o.s. (including C2-C12 homologues)
2431	153	Anisidines
2432	153	N,N-Diethylaniline
2433	152	Chloronitrotoluenes, liquid
2434	156	Dibenzyldichlorosilane
2435	156	Ethylphenyldichlorosilane
2436	129	Thioacetic acid
2437	156	Methylphenyldichlorosilane
2438	131	Trimethylacetyl chloride
2439	154	Sodium hydrogendifluoride
2440	154	Stannic chloride, pentahydrate
2441	135	Titanium trichloride, pyrophoric
2441	135	Titanium trichloride mixture, pyrophoric
2442	156	Trichloroacetyl chloride
2443	137	Vanadium oxytrichloride
2444	137	Vanadium tetrachloride
2446	153	Nitrocresols, solid
2447	136	Phosphorus, white, molten
2447	136	White phosphorus, molten
2448	133	Molten sulfur
2448	133	Molten sulphur
2448	133	Sulfur, molten
2448	133	Sulphur, molten
2451	122	Nitrogen trifluoride
2451	122	Nitrogen trifluoride, compressed
2452	116P	Ethylacetylene, stabilized
2453	115	Ethyl fluoride
2453	115	Refrigerant gas R-161
2454	115	Methyl fluoride
2454	115	Refrigerant gas R-41
2455	116	Methyl nitrite
2456	130P	2-Chloropropene
2457	128	2,3-Dimethylbutane
2458	130	Hexadiene
2459	128	2-Methyl-1-butene
2460	128	2-Methyl-2-butene
2461	128	Methylpentadiene
2463	138	Aluminum hydride
2464	141	Beryllium nitrate
2465	140	Dichloroisocyanuric acid, dry
2465	140	Dichloroisocyanuric acid salts
2465	140	Sodium dichloroisocyanurate
2465	140	Sodium dichloro-s-triazinetrione
2466	143	Potassium superoxide
2468	140	Trichloroisocyanuric acid, dry
2469	140	Zinc bromate
2470	152	Phenylacetonitrile, liquid
2471	154	Osmium tetroxide
2473	154	Sodium arsanilate
2474	157	Thiophosgene
2475	157	Vanadium trichloride
2477	131	Methyl isothiocyanate
2478	155	Isocyanate solution, flammable, poisonous, n.o.s.
2478	155	Isocyanate solution, flammable, toxic, n.o.s.
2478	155	Isocyanates, flammable, poisonous, n.o.s.

ID No.	Guide No.	Name of Material
2478	155	Isocyanates, flammable, toxic, n.o.s.
2480	155P	Methyl isocyanate
2481	155	Ethyl isocyanate
2482	155P	n-Propyl isocyanate
2483	155P	Isopropyl isocyanate
2484	155	tert-Butyl isocyanate
2485	155P	n-Butyl isocyanate
2486	155P	Isobutyl isocyanate
2487	155	Phenyl isocyanate
2488	155	Cyclohexyl isocyanate
2490	153	Dichloroisopropyl ether
2491	153	Ethanolamine
2491	153	Ethanolamine, solution
2491	153	Monoethanolamine
2493	132	Hexamethyleneimine
2495	144	Iodine pentafluoride
2496	156	Propionic anhydride
2498	129	1,2,3,6-Tetrahydrobenzaldehyde
2501	152	Tris-(1-aziridinyl)phosphine oxide, solution
2502	132	Valeryl chloride
2503	137	Zirconium tetrachloride
2504	159	Acetylene tetrabromide
2504	159	Tetrabromoethane
2505	154	Ammonium fluoride
2506	154	Ammonium hydrogen sulfate
2506	154	Ammonium hydrogen sulphate
2507	154	Chloroplatinic acid, solid
2508	156	Molybdenum pentachloride
2509	154	Potassium hydrogen sulfate
2509	154	Potassium hydrogen sulphate

ID No.	Guide No.	Name of Material
2511	153	2-Chloropropionic acid
2512	152	Aminophenols
2513	156	Bromoacetyl bromide
2514	130	Bromobenzene
2515	159	Bromoform
2516	151	Carbon tetrabromide
2517	115	1-Chloro-1,1-difluoroethane
2517	115	Difluorochloroethanes
2517	115	Refrigerant gas R-142b
2518	153	1,5,9-Cyclododecatriene
2520	130P	Cyclooctadienes
2521	131P	Diketene, stabilized
2522	153P	2-Dimethylaminoethyl methacrylate
2524	129	Ethyl orthoformate
2525	156	Ethyl oxalate
2526	132	Furfurylamine
2527	129P	Isobutyl acrylate, stabilized
2528	130	Isobutyl isobutyrate
2529	132	Isobutyric acid
2531	153P	Methacrylic acid, stabilized
2533	156	Methyl trichloroacetate
2534	119	Methylchlorosilane
2535	132	4-Methylmorpholine
2535	132	N-Methylmorpholine
2536	127	Methyltetrahydrofuran
2538	133	Nitronaphthalene
2541	128	Terpinolene
2542	153	Tributylamine
2545	135	Hafnium powder, dry
2546	135	Titanium powder, dry
2547	143	Sodium superoxide

ID No.	Guide No.	Name of Material
2548	124	Chlorine pentafluoride
2552	151	Hexafluoroacetone hydrate, liquid
2554	130P	Methylallyl chloride
2555	113	Nitrocellulose with water, not less than 25% water
2556	113	Nitrocellulose with alcohol, not less than 25% alcohol
2557	133	Nitrocellulose mixture, without pigment
2557	133	Nitrocellulose mixture, without plasticizer
2557	133	Nitrocellulose mixture, with pigment
2557	133	Nitrocellulose mixture, with plasticizer
2558	131	Epibromohydrin
2560	129	2-Methylpentan-2-ol
2561	128	3-Methyl-1-butene
2564	153	Trichloroacetic acid, solution
2565	153	Dicyclohexylamine
2567	154	Sodium pentachlorophenate
2570	154	Cadmium compound
2571	156	Alkylsulfuric acids
2571	156	Alkylsulphuric acids
2572	153	Phenylhydrazine
2573	141	Thallium chlorate
2574	151	Tricresyl phosphate
2576	137	Phosphorus oxybromide, molten
2577	156	Phenylacetyl chloride
2578	157	Phosphorus trioxide
2579	153	Piperazine
2580	154	Aluminum bromide, solution
2581	154	Aluminum chloride, solution
2582	154	Ferric chloride, solution
2583	153	Alkyl sulfonic acids, solid, with more than 5% free Sulfuric acid
2583	153	Alkyl sulphonic acids, solid, with more than 5% free Sulphuric acid
2583	153	Aryl sulfonic acids, solid, with more than 5% free Sulfuric acid
2583	153	Aryl sulphonic acids, solid, with more than 5% free Sulphuric acid
2584	153	Alkyl sulfonic acids, liquid, with more than 5% free Sulfuric acid
2584	153	Alkyl sulphonic acids, liquid, with more than 5% free Sulphuric acid
2584	153	Aryl sulfonic acids, liquid, with more than 5% free Sulfuric acid
2584	153	Aryl sulphonic acids, liquid, with more than 5% free Sulphuric acid
2585	153	Alkyl sulfonic acids, solid, with not more than 5% free Sulfuric acid
2585	153	Alkyl sulphonic acids, solid, with not more than 5% free Sulphuric acid
2585	153	Aryl sulfonic acids, solid, with not more than 5% free Sulfuric acid
2585	153	Aryl sulphonic acids, solid, with not more than 5% free Sulphuric acid
2586	153	Alkyl sulfonic acids, liquid, with not more than 5% free Sulfuric acid
2586	153	Alkyl sulphonic acids, liquid, with not more than 5% free Sulphuric acid

ID No.	Guide No.	Name of Material
2586	153	Aryl sulfonic acids, liquid, with not more than 5% free Sulfuric acid
2586	153	Aryl sulphonic acids, liquid, with not more than 5% free Sulphuric acid
2587	153	Benzoquinone
2588	151	Pesticide, solid, poisonous, n.o.s.
2588	151	Pesticide, solid, toxic, n.o.s.
2589	155	Vinyl chloroacetate
2590	171	Asbestos, chrysotile
2590	171	Asbestos, white
2590	171	White asbestos
2591	120	Xenon, refrigerated liquid (cryogenic liquid)
2599	126	Chlorotrifluoromethane and Trifluoromethane azeotropic mixture with approximately 60% Chlorotrifluoromethane
2599	126	Refrigerant gas R-503
2599	126	Trifluoromethane and Chlorotrifluoromethane azeotropic mixture with approximately 60% Chlorotrifluoromethane
2601	115	Cyclobutane
2602	126	Dichlorodifluoromethane and Difluoroethane azeotropic mixture with approximately 74% Dichlorodifluoromethane
2602	126	Difluoroethane and Dichlorodifluoromethane azeotropic mixture with approximately 74% Dichlorodifluoromethane
2602	126	Refrigerant gas R-500
2603	131	Cycloheptatriene
2604	132	Boron trifluoride diethyl etherate
2605	155	Methoxymethyl isocyanate
2606	155	Methyl orthosilicate
2607	129P	Acrolein dimer, stabilized
2608	129	Nitropropanes
2609	156	Triallyl borate
2610	132	Triallylamine
2611	131	Propylene chlorohydrin
2612	127	Methyl propyl ether
2614	129	Methallyl alcohol
2615	127	Ethyl propyl ether
2616	129	Triisopropyl borate
2617	129	Methylcyclohexanols
2618	130P	Vinyltoluenes, stabilized
2619	132	Benzyldimethylamine
2620	130	Amyl butyrates
2621	127	Acetyl methyl carbinol
2622	131P	Glycidaldehyde
2623	133	Firelighters, solid, with flammable liquid
2624	138	Magnesium silicide
2626	140	Chloric acid, aqueous solution, with not more than 10% Chloric acid
2627	140	Nitrites, inorganic, n.o.s.
2628	151	Potassium fluoroacetate
2629	151	Sodium fluoroacetate
2630	151	Selenates
2630	151	Selenites
2642	154	Fluoroacetic acid
2643	155	Methyl bromoacetate
2644	151	Methyl iodide
2645	153	Phenacyl bromide

ID No.	Guide No.	Name of Material
2646	151	Hexachlorocyclopentadiene
2647	153	Malononitrile
2648	154	1,2-Dibromobutan-3-one
2649	153	1,3-Dichloroacetone
2650	153	1,1-Dichloro-1-nitroethane
2651	153	4,4'-Diaminodiphenylmethane
2653	156	Benzyl iodide
2655	151	Potassium fluorosilicate
2656	154	Quinoline
2657	153	Selenium disulfide
2657	153	Selenium disulphide
2659	151	Sodium chloroacetate
2660	153	Mononitrotoluidines
2660	153	Nitrotoluidines (mono)
2661	153	Hexachloroacetone
2664	160	Dibromomethane
2667	152	Butyltoluenes
2668	131	Chloroacetonitrile
2669	152	Chlorocresols, solution
2670	157	Cyanuric chloride
2671	153	Aminopyridines
2672	154	Ammonia, solution, with more than 10% but not more than 35% Ammonia
2672	154	Ammonium hydroxide
2672	154	Ammonium hydroxide, with more than 10% but not more than 35% Ammonia
2673	151	2-Amino-4-chlorophenol
2674	154	Sodium fluorosilicate
2676	119	Stibine
2677	154	Rubidium hydroxide, solution
2678	154	Rubidium hydroxide, solid
2679	154	Lithium hydroxide, solution
2680	154	Lithium hydroxide
2681	154	Caesium hydroxide, solution
2681	154	Cesium hydroxide, solution
2682	157	Caesium hydroxide
2682	157	Cesium hydroxide
2683	132	Ammonium sulfide, solution
2683	132	Ammonium sulphide, solution
2684	132	3-Diethylaminopropylamine
2685	132	N,N-Diethylethylenediamine
2686	132	2-Diethylaminoethanol
2687	133	Dicyclohexylammonium nitrite
2688	159	1-Bromo-3-chloropropane
2689	153	Glycerol alpha-monochlorohydrin
2690	152	N,n-Butylimidazole
2691	137	Phosphorus pentabromide
2692	157	Boron tribromide
2693	154	Bisulfites, aqueous solution, n.o.s.
2693	154	Bisulphites, aqueous solution, n.o.s.
2698	156	Tetrahydrophthalic anhydrides
2699	154	Trifluoroacetic acid
2705	153P	1-Pentol
2707	127	Dimethyldioxanes
2709	128	Butylbenzenes
2710	128	Dipropyl ketone
2713	153	Acridine
2714	133	Zinc resinate
2715	133	Aluminum resinate
2716	153	1,4-Butynediol

ID No.	Guide No.	Name of Material
2717	133	Camphor, synthetic
2719	141	Barium bromate
2720	141	Chromium nitrate
2721	140	Copper chlorate
2722	140	Lithium nitrate
2723	140	Magnesium chlorate
2724	140	Manganese nitrate
2725	140	Nickel nitrate
2726	140	Nickel nitrite
2727	141	Thallium nitrate
2728	140	Zirconium nitrate
2729	152	Hexachlorobenzene
2730	152	Nitroanisoles, liquid
2732	152	Nitrobromobenzenes, liquid
2733	132	Amines, flammable, corrosive, n.o.s.
2733	132	Polyamines, flammable, corrosive, n.o.s.
2734	132	Amines, liquid, corrosive, flammable, n.o.s.
2734	132	Polyamines, liquid, corrosive, flammable, n.o.s.
2735	153	Amines, liquid, corrosive, n.o.s.
2735	153	Polyamines, liquid, corrosive, n.o.s.
2738	153	N-Butylaniline
2739	156	Butyric anhydride
2740	155	n-Propyl chloroformate
2741	141	Barium hypochlorite, with more than 22% available Chlorine
2742	155	sec-Butyl chloroformate
2742	155	Chloroformates, poisonous, corrosive, flammable, n.o.s.
2742	155	Chloroformates, toxic, corrosive, flammable, n.o.s.
2742	155	Isobutyl chloroformate
2743	155	n-Butyl chloroformate
2744	155	Cyclobutyl chloroformate
2745	157	Chloromethyl chloroformate
2746	156	Phenyl chloroformate
2747	156	tert-Butylcyclohexyl chloroformate
2748	156	2-Ethylhexyl chloroformate
2749	130	Tetramethylsilane
2750	153	1,3-Dichloropropanol-2
2751	155	Diethylthiophosphoryl chloride
2752	127	1,2-Epoxy-3-ethoxypropane
2753	153	N-Ethylbenzyltoluidines, liquid
2754	153	N-Ethyltoluidines
2757	151	Carbamate pesticide, solid, poisonous
2757	151	Carbamate pesticide, solid, toxic
2758	131	Carbamate pesticide, liquid, flammable, poisonous
2758	131	Carbamate pesticide, liquid, flammable, toxic
2759	151	Arsenical pesticide, solid, poisonous
2759	151	Arsenical pesticide, solid, toxic
2760	131	Arsenical pesticide, liquid, flammable, poisonous
2760	131	Arsenical pesticide, liquid, flammable, toxic
2761	151	Organochlorine pesticide, solid, poisonous
2761	151	Organochlorine pesticide, solid, toxic

ID No.	Guide No.	Name of Material
2762	131	Organochlorine pesticide, liquid, flammable, poisonous
2762	131	Organochlorine pesticide, liquid, flammable, toxic
2763	151	Triazine pesticide, solid, poisonous
2763	151	Triazine pesticide, solid, toxic
2764	131	Triazine pesticide, liquid, flammable, poisonous
2764	131	Triazine pesticide, liquid, flammable, toxic
2771	151	Thiocarbamate pesticide, solid, poisonous
2771	151	Thiocarbamate pesticide, solid, toxic
2772	131	Thiocarbamate pesticide, liquid, flammable, poisonous
2772	131	Thiocarbamate pesticide, liquid, flammable, toxic
2775	151	Copper based pesticide, solid, poisonous
2775	151	Copper based pesticide, solid, toxic
2776	131	Copper based pesticide, liquid, flammable, poisonous
2776	131	Copper based pesticide, liquid, flammable, toxic
2777	151	Mercury based pesticide, solid, poisonous
2777	151	Mercury based pesticide, solid, toxic
2778	131	Mercury based pesticide, liquid, flammable, poisonous
2778	131	Mercury based pesticide, liquid, flammable, toxic
2779	153	Substituted nitrophenol pesticide, solid, poisonous
2779	153	Substituted nitrophenol pesticide, solid, toxic
2780	131	Substituted nitrophenol pesticide, liquid, flammable, poisonous
2780	131	Substituted nitrophenol pesticide, liquid, flammable, toxic
2781	151	Bipyridilium pesticide, solid, poisonous
2781	151	Bipyridilium pesticide, solid, toxic
2782	131	Bipyridilium pesticide, liquid, flammable, poisonous
2782	131	Bipyridilium pesticide, liquid, flammable, toxic
2783	152	Organophosphorus pesticide, solid, poisonous
2783	152	Organophosphorus pesticide, solid, toxic
2784	131	Organophosphorus pesticide, liquid, flammable, poisonous
2784	131	Organophosphorus pesticide, liquid, flammable, toxic
2785	152	4-Thiapentanal
2786	153	Organotin pesticide, solid, poisonous
2786	153	Organotin pesticide, solid, toxic
2787	131	Organotin pesticide, liquid, flammable, poisonous
2787	131	Organotin pesticide, liquid, flammable, toxic
2788	153	Organotin compound, liquid, n.o.s.
2789	132	Acetic acid, glacial
2789	132	Acetic acid, solution, more than 80% acid
2790	153	Acetic acid, solution, more than 10% but not more than 80% acid

ID No.	Guide No.	Name of Material
2793	170	Ferrous metal borings, shavings, turnings or cuttings
2794	154	Batteries, wet, filled with acid
2795	154	Batteries, wet, filled with alkali
2796	157	Battery fluid, acid
2796	157	Sulfuric acid, with not more than 51% acid
2796	157	Sulphuric acid, with not more than 51% acid
2797	154	Battery fluid, alkali
2798	137	Benzene phosphorus dichloride
2798	137	Phenylphosphorus dichloride
2799	137	Benzene phosphorus thiodichloride
2799	137	Phenylphosphorus thiodichloride
2800	154	Batteries, wet, non-spillable
2801	154	Dye, liquid, corrosive, n.o.s.
2801	154	Dye intermediate, liquid, corrosive, n.o.s.
2802	154	Copper chloride
2803	172	Gallium
2805	138	Lithium hydride, fused solid
2806	139	Lithium nitride
2807	171	Magnetized material
2809	172	Mercury
2810	153	Compounds, tree or weed killing, liquid (toxic)
2810	153	Poisonous liquid, organic, n.o.s.
2810	153	Toxic liquid, organic, n.o.s.
2811	154	Poisonous solid, organic, n.o.s.
2811	154	Toxic solid, organic, n.o.s.
2812	154	Sodium aluminate, solid
2813	138	Water-reactive solid, n.o.s.
2814	158	Infectious substance, affecting humans
2815	153	N-Aminoethylpiperazine
2817	154	Ammonium bifluoride, solution
2817	154	Ammonium hydrogendifluoride, solution
2818	154	Ammonium polysulfide, solution
2818	154	Ammonium polysulphide, solution
2819	153	Amyl acid phosphate
2820	153	Butyric acid
2821	153	Phenol solution
2822	153	2-Chloropyridine
2823	153	Crotonic acid, solid
2826	155	Ethyl chlorothioformate
2829	153	Caproic acid
2829	153	Hexanoic acid
2830	139	Lithium ferrosilicon
2831	160	1,1,1-Trichloroethane
2834	154	Phosphorous acid
2835	138	Sodium aluminum hydride
2837	154	Bisulfates, aqueous solution
2837	154	Bisulphates, aqueous solution
2837	154	Sodium bisulfate, solution
2837	154	Sodium bisulphate, solution
2838	129P	Vinyl butyrate, stabilized
2839	153	Aldol
2840	129	Butyraldoxime
2841	131	Di-n-amylamine
2842	129	Nitroethane
2844	138	Calcium manganese silicon
2845	135	Ethyl phosphonous dichloride, anhydrous

ID No.	Guide No.	Name of Material
2845	135	Methyl phosphonous dichloride
2845	135	Pyrophoric liquid, organic, n.o.s.
2846	135	Pyrophoric solid, organic, n.o.s.
2849	153	3-Chloropropanol-1
2850	128	Propylene tetramer
2851	157	Boron trifluoride, dihydrate
2852	113	Dipicryl sulfide, wetted with not less than 10% water
2852	113	Dipicryl sulphide, wetted with not less than 10% water
2853	151	Magnesium fluorosilicate
2854	151	Ammonium fluorosilicate
2854	151	Ammonium silicofluoride
2855	151	Zinc fluorosilicate
2855	151	Zinc silicofluoride
2856	151	Fluorosilicates, n.o.s.
2857	126	Refrigerating machines, containing Ammonia solutions (UN2672)
2857	126	Refrigerating machines, containing non-flammable, non-poisonous gases
2857	126	Refrigerating machines, containing non-flammable, non-toxic gases
2858	170	Zirconium, dry, coiled wire, finished metal sheets or strip
2859	154	Ammonium metavanadate
2861	151	Ammonium polyvanadate
2862	151	Vanadium pentoxide
2863	154	Sodium ammonium vanadate
2864	151	Potassium metavanadate
2865	154	Hydroxylamine sulfate
2865	154	Hydroxylamine sulphate
2869	157	Titanium trichloride mixture
2870	135	Aluminum borohydride
2870	135	Aluminum borohydride in devices
2871	170	Antimony powder
2872	159	Dibromochloropropanes
2873	153	Dibutylaminoethanol
2874	153	Furfuryl alcohol
2875	151	Hexachlorophene
2876	153	Resorcinol
2878	170	Titanium sponge granules
2878	170	Titanium sponge powders
2879	157	Selenium oxychloride
2880	140	Calcium hypochlorite, hydrated, with not less than 5.5% but not more than 16% water
2880	140	Calcium hypochlorite, hydrated mixture, with not less than 5.5% but not more than 16% water
2881	135	Metal catalyst, dry
2881	135	Nickel catalyst, dry
2900	158	Infectious substance, affecting animals only
2901	124	Bromine chloride
2902	151	Pesticide, liquid, poisonous, n.o.s.
2902	151	Pesticide, liquid, toxic, n.o.s.
2903	131	Pesticide, liquid, poisonous, flammable, n.o.s.
2903	131	Pesticide, liquid, toxic, flammable, n.o.s.
2904	154	Chlorophenolates, liquid
2904	154	Phenolates, liquid
2905	154	Chlorophenolates, solid

ID No.	Guide No.	Name of Material
2905	154	Phenolates, solid
2907	133	Isosorbide dinitrate mixture
2908	161	Radioactive material, excepted package, empty packaging
2909	161	Radioactive material, excepted package, articles manufactured from depleted Uranium
2909	161	Radioactive material, excepted package, articles manufactured from natural Thorium
2909	161	Radioactive material, excepted package, articles manufactured from natural Uranium
2910	161	Radioactive material, excepted package, limited quantity of material
2911	161	Radioactive material, excepted package, articles
2911	161	Radioactive material, excepted package, instruments
2912	162	Radioactive material, low specific activity (LSA-I), non fissile or fissile-excepted
2913	162	Radioactive material, surface contaminated objects (SCO-I), non fissile or fissile-excepted
2913	162	Radioactive material, surface contaminated objects (SCO-II), non fissile or fissile-excepted
2915	163	Radioactive material, Type A package, non-special form, non fissile or fissile-excepted
2916	163	Radioactive material, Type B(U) package, non fissile or fissile-excepted
2917	163	Radioactive material, Type B(M) package, non fissile or fissile-excepted
2919	163	Radioactive material, transported under special arrangement, non fissile or fissile-excepted
2920	132	Corrosive liquid, flammable, n.o.s.
2921	134	Corrosive solid, flammable, n.o.s.
2922	154	Corrosive liquid, poisonous, n.o.s.
2922	154	Corrosive liquid, toxic, n.o.s.
2923	154	Corrosive solid, poisonous, n.o.s.
2923	154	Corrosive solid, toxic, n.o.s.
2924	132	Flammable liquid, corrosive, n.o.s
2925	134	Flammable solid, corrosive, organic, n.o.s.
2926	134	Flammable solid, poisonous, organic, n.o.s.
2926	134	Flammable solid, toxic, organic, n.o.s.
2927	154	Ethyl phosphonothioic dichloride, anhydrous
2927	154	Ethyl phosphorodichloridate
2927	154	Poisonous liquid, corrosive, organic, n.o.s.
2927	154	Toxic liquid, corrosive, organic, n.o.s.
2928	154	Poisonous solid, corrosive, organic, n.o.s.
2928	154	Toxic solid, corrosive, organic, n.o.s.
2929	131	Poisonous liquid, flammable, organic, n.o.s.
2929	131	Toxic liquid, flammable, organic, n.o.s.
2930	134	Poisonous solid, flammable, organic, n.o.s.

ID No.	Guide No.	Name of Material
2930	134	Toxic solid, flammable, organic, n.o.s.
2931	151	Vanadyl sulfate
2931	151	Vanadyl sulphate
2933	129	Methyl 2-chloropropionate
2934	129	Isopropyl 2-chloropropionate
2935	129	Ethyl 2-chloropropionate
2936	153	Thiolactic acid
2937	153	alpha-Methylbenzyl alcohol, liquid
2937	153	Methylbenzyl (alpha) alcohol, liquid
2940	135	Cyclooctadiene phosphines
2940	135	9-Phosphabicyclononanes
2941	153	Fluoroanilines
2942	153	2-Trifluoromethylaniline
2943	129	Tetrahydrofurfurylamine
2945	132	N-Methylbutylamine
2946	153	2-Amino-5-diethylaminopentane
2947	155	Isopropyl chloroacetate
2948	153	3-Trifluoromethylaniline
2949	154	Sodium hydrosulfide, hydrated, with not less than 25% water of crystallization
2949	154	Sodium hydrosulfide, with not less than 25% water of crystallization
2949	154	Sodium hydrosulphide, hydrated, with not less than 25% water of crystallization
2949	154	Sodium hydrosulphide, with not less than 25% water of crystallization
2950	138	Magnesium granules, coated
2956	149	5-tert-Butyl-2,4,6-trinitro-m-xylene
2956	149	Musk xylene
2965	139	Boron trifluoride dimethyl etherate
2966	153	Thioglycol
2967	154	Sulfamic acid
2967	154	Sulphamic acid
2968	135	Maneb, stabilized
2968	135	Maneb preparation, stabilized
2969	171	Castor beans, meal, pomace or flake
2977	166	Radioactive material, Uranium hexafluoride, fissile
2977	166	Uranium hexafluoride, radioactive material, fissile
2978	166	Radioactive material, Uranium hexafluoride, non fissile or fissile-excepted
2978	166	Uranium hexafluoride, radioactive material, non fissile or fissile-excepted
2983	131P	Ethylene oxide and Propylene oxide mixture, with not more than 30% Ethylene oxide
2983	131P	Propylene oxide and Ethylene oxide mixture, with not more than 30% Ethylene oxide
2984	140	Hydrogen peroxide, aqueous solution, with not less than 8% but less than 20% Hydrogen peroxide
2985	155	Chlorosilanes, flammable, corrosive, n.o.s.
2986	155	Chlorosilanes, corrosive, flammable, n.o.s.
2987	156	Chlorosilanes, corrosive, n.o.s.
2988	139	Chlorosilanes, water-reactive, flammable, corrosive, n.o.s.
2989	133	Lead phosphite, dibasic

ID No.	Guide No.	Name of Material
2990	171	Life-saving appliances, self-inflating
2991	131	Carbamate pesticide, liquid, poisonous, flammable
2991	131	Carbamate pesticide, liquid, toxic, flammable
2992	151	Carbamate pesticide, liquid, poisonous
2992	151	Carbamate pesticide, liquid, toxic
2993	131	Arsenical pesticide, liquid, poisonous, flammable
2993	131	Arsenical pesticide, liquid, toxic, flammable
2994	151	Arsenical pesticide, liquid, poisonous
2994	151	Arsenical pesticide, liquid, toxic
2995	131	Organochlorine pesticide, liquid, poisonous, flammable
2995	131	Organochlorine pesticide, liquid, toxic, flammable
2996	151	Organochlorine pesticide, liquid, poisonous
2996	151	Organochlorine pesticide, liquid, toxic
2997	131	Triazine pesticide, liquid, poisonous, flammable
2997	131	Triazine pesticide, liquid, toxic, flammable
2998	151	Triazine pesticide, liquid, poisonous
2998	151	Triazine pesticide, liquid, toxic
3002	151	Phenyl urea pesticide, liquid, poisonous
3002	151	Phenyl urea pesticide, liquid, toxic
3005	131	Thiocarbamate pesticide, liquid, poisonous, flammable
3005	131	Thiocarbamate pesticide, liquid, toxic, flammable
3006	151	Thiocarbamate pesticide, liquid, poisonous
3006	151	Thiocarbamate pesticide, liquid, toxic
3009	131	Copper based pesticide, liquid, poisonous, flammable
3009	131	Copper based pesticide, liquid, toxic, flammable
3010	151	Copper based pesticide, liquid, poisonous
3010	151	Copper based pesticide, liquid, toxic
3011	131	Mercury based pesticide, liquid, poisonous, flammable
3011	131	Mercury based pesticide, liquid, toxic, flammable
3012	151	Mercury based pesticide, liquid, poisonous
3012	151	Mercury based pesticide, liquid, toxic
3013	131	Substituted nitrophenol pesticide, liquid, poisonous, flammable
3013	131	Substituted nitrophenol pesticide, liquid, toxic, flammable
3014	153	Substituted nitrophenol pesticide, liquid, poisonous
3014	153	Substituted nitrophenol pesticide, liquid, toxic
3015	131	Bipyridilium pesticide, liquid, poisonous, flammable
3015	131	Bipyridilium pesticide, liquid, toxic, flammable
3016	151	Bipyridilium pesticide, liquid, poisonous
3016	151	Bipyridilium pesticide, liquid, toxic

ID No.	Guide No.	Name of Material
3017	131	Organophosphorus pesticide, liquid, poisonous, flammable
3017	131	Organophosphorus pesticide, liquid, toxic, flammable
3018	152	Organophosphorus pesticide, liquid, poisonous
3018	152	Organophosphorus pesticide, liquid, toxic
3019	131	Organotin pesticide, liquid, poisonous, flammable
3019	131	Organotin pesticide, liquid, toxic, flammable
3020	153	Organotin pesticide, liquid, poisonous
3020	153	Organotin pesticide, liquid, toxic
3021	131	Pesticide, liquid, flammable, poisonous, n.o.s.
3021	131	Pesticide, liquid, flammable, toxic, n.o.s.
3022	127P	1,2-Butylene oxide, stabilized
3023	131	2-Methyl-2-heptanethiol
3024	131	Coumarin derivative pesticide, liquid, flammable, poisonous
3024	131	Coumarin derivative pesticide, liquid, flammable, toxic
3025	131	Coumarin derivative pesticide, liquid, poisonous, flammable
3025	131	Coumarin derivative pesticide, liquid, toxic, flammable
3026	151	Coumarin derivative pesticide, liquid, poisonous
3026	151	Coumarin derivative pesticide, liquid, toxic
3027	151	Coumarin derivative pesticide, solid, poisonous
3027	151	Coumarin derivative pesticide, solid, toxic
3028	154	Batteries, dry, containing Potassium hydroxide solid
3048	157	Aluminum phosphide pesticide
3051	135	Aluminum alkyls
3053	135	Magnesium alkyls
3054	129	Cyclohexanethiol
3054	129	Cyclohexyl mercaptan
3055	154	2-(2-Aminoethoxy)ethanol
3056	129	n-Heptaldehyde
3057	125	Trifluoroacetyl chloride
3064	127	Nitroglycerin, solution in alcohol, with more than 1% but not more than 5% Nitroglycerin
3065	127	Alcoholic beverages
3066	153	Paint (corrosive)
3066	153	Paint related material (corrosive)
3070	126	Dichlorodifluoromethane and Ethylene oxide mixture, with not more than 12.5% Ethylene oxide
3070	126	Ethylene oxide and Dichlorodifluoromethane mixture, with not more than 12.5% Ethylene oxide
3071	131	Mercaptan mixture, liquid, poisonous, flammable, n.o.s.
3071	131	Mercaptan mixture, liquid, toxic, flammable, n.o.s.
3071	131	Mercaptans, liquid, poisonous, flammable, n.o.s.
3071	131	Mercaptans, liquid, toxic, flammable, n.o.s.
3072	171	Life-saving appliances, not self-inflating
3073	131P	Vinylpyridines, stabilized
3076	138	Aluminum alkyl hydrides
3077	171	Environmentally hazardous substance, solid, n.o.s.

ID No.	Guide No.	Name of Material
3077	171	Hazardous waste, solid, n.o.s.
3077	171	Other regulated substances, solid, n.o.s.
3078	138	Cerium, turnings or gritty powder
3079	131P	Methacrylonitrile, stabilized
3080	155	Isocyanate solution, poisonous, flammable, n.o.s.
3080	155	Isocyanate solution, toxic, flammable, n.o.s.
3080	155	Isocyanates, poisonous, flammable, n.o.s.
3080	155	Isocyanates, toxic, flammable, n.o.s.
3082	171	Environmentally hazardous substance, liquid, n.o.s.
3082	171	Hazardous waste, liquid, n.o.s.
3082	171	Other regulated substances, liquid, n.o.s.
3083	124	Perchloryl fluoride
3084	157	Corrosive solid, oxidizing, n.o.s.
3085	140	Oxidizing solid, corrosive, n.o.s.
3086	141	Poisonous solid, oxidizing, n.o.s.
3086	141	Toxic solid, oxidizing, n.o.s.
3087	141	Oxidizing solid, poisonous, n.o.s.
3087	141	Oxidizing solid, toxic, n.o.s.
3088	135	Self-heating solid, organic, n.o.s.
3089	170	Metal powder, flammable, n.o.s.
3090	138	Lithium batteries
3090	138	Lithium metal batteries (including lithium alloy batteries)
3091	138	Lithium batteries contained in equipment
3091	138	Lithium batteries packed with equipment
3091	138	Lithium metal batteries contained in equipment (including lithium alloy batteries)
3091	138	Lithium metal batteries packed with equipment (including lithium alloy batteries)
3092	129	1-Methoxy-2-propanol
3093	157	Corrosive liquid, oxidizing, n.o.s.
3094	138	Corrosive liquid, water-reactive, n.o.s.
3095	136	Corrosive solid, self-heating, n.o.s.
3096	138	Corrosive solid, water-reactive, n.o.s.
3097	140	Flammable solid, oxidizing, n.o.s.
3098	140	Oxidizing liquid, corrosive, n.o.s.
3099	142	Oxidizing liquid, poisonous, n.o.s.
3099	142	Oxidizing liquid, toxic, n.o.s.
3100	135	Oxidizing solid, self-heating, n.o.s.
3101	146	Organic peroxide type B, liquid
3102	146	Organic peroxide type B, solid
3103	146	Organic peroxide type C, liquid
3104	146	Organic peroxide type C, solid
3105	145	Organic peroxide type D, liquid
3106	145	Organic peroxide type D, solid
3107	145	Organic peroxide type E, liquid
3108	145	Organic peroxide type E, solid
3109	145	Organic peroxide type F, liquid
3110	145	Organic peroxide type F, solid

ID No.	Guide No.	Name of Material
3111	**148**	Organic peroxide type B, liquid, temperature controlled
3112	**148**	Organic peroxide type B, solid, temperature controlled
3113	**148**	Organic peroxide type C, liquid, temperature controlled
3114	**148**	Organic peroxide type C, solid, temperature controlled
3115	**148**	Organic peroxide type D, liquid, temperature controlled
3116	**148**	Organic peroxide type D, solid, temperature controlled
3117	**148**	Organic peroxide type E, liquid, temperature controlled
3118	**148**	Organic peroxide type E, solid, temperature controlled
3119	**148**	Organic peroxide type F, liquid, temperature controlled
3120	**148**	Organic peroxide type F, solid, temperature controlled
3121	**144**	Oxidizing solid, water-reactive, n.o.s.
3122	**142**	Poisonous liquid, oxidizing, n.o.s.
3122	**142**	Toxic liquid, oxidizing, n.o.s.
3123	**139**	Poisonous liquid, water-reactive, n.o.s.
3123	**139**	Toxic liquid, water-reactive, n.o.s.
3124	**136**	Poisonous solid, self-heating, n.o.s.
3124	**136**	Toxic solid, self-heating, n.o.s.
3125	**139**	Poisonous solid, water-reactive, n.o.s.
3125	**139**	Toxic solid, water-reactive, n.o.s.
3126	**136**	Self-heating solid, corrosive, organic, n.o.s.
3127	**135**	Self-heating solid, oxidizing, n.o.s.
3128	**136**	Self-heating solid, poisonous, organic, n.o.s.
3128	**136**	Self-heating solid, toxic, organic, n.o.s.
3129	**138**	Water-reactive liquid, corrosive, n.o.s.
3130	**139**	Water-reactive liquid, poisonous, n.o.s.
3130	**139**	Water-reactive liquid, toxic, n.o.s.
3131	**138**	Water-reactive solid, corrosive, n.o.s.
3132	**138**	Water-reactive solid, flammable, n.o.s.
3133	**138**	Water-reactive solid, oxidizing, n.o.s.
3134	**139**	Water-reactive solid, poisonous, n.o.s.
3134	**139**	Water-reactive solid, toxic, n.o.s.
3135	**138**	Water-reactive solid, self-heating, n.o.s.
3136	**120**	Trifluoromethane, refrigerated liquid
3137	**140**	Oxidizing solid, flammable, n.o.s.
3138	**115**	Acetylene, Ethylene and Propylene in mixture, refrigerated liquid containing at least 71.5% Ethylene with not more than 22.5% Acetylene and not more than 6% Propylene
3138	**115**	Ethylene, Acetylene and Propylene in mixture, refrigerated liquid containing at least 71.5% Ethylene with not more than 22.5% Acetylene and not more than 6% Propylene

ID No.	Guide No.	Name of Material
3138	115	Propylene, Ethylene and Acetylene in mixture, refrigerated liquid containing at least 71.5% Ethylene with not more than 22.5% Acetylene and not more than 6% Propylene
3139	140	Oxidizing liquid, n.o.s.
3140	151	Alkaloids, liquid, n.o.s. (poisonous)
3140	151	Alkaloid salts, liquid, n.o.s. (poisonous)
3141	157	Antimony compound, inorganic, liquid, n.o.s.
3142	151	Disinfectant, liquid, poisonous, n.o.s.
3142	151	Disinfectant, liquid, toxic, n.o.s.
3143	151	Dye, solid, poisonous, n.o.s.
3143	151	Dye, solid, toxic, n.o.s.
3143	151	Dye intermediate, solid, poisonous, n.o.s.
3143	151	Dye intermediate, solid, toxic, n.o.s.
3144	151	Nicotine compound, liquid, n.o.s.
3144	151	Nicotine preparation, liquid, n.o.s.
3145	153	Alkylphenols, liquid, n.o.s. (including C2-C12 homologues)
3146	153	Organotin compound, solid, n.o.s.
3147	154	Dye, solid, corrosive, n.o.s.
3147	154	Dye intermediate, solid, corrosive, n.o.s.
3148	138	Water-reactive liquid, n.o.s.
3149	140	Hydrogen peroxide and Peroxyacetic acid mixture, with acid(s), water and not more than 5% Peroxyacetic acid, stabilized
3149	140	Peroxyacetic acid and hydrogen peroxide mixture, with acid(s), water and not more than 5% Peroxyacetic acid, stabilized
3150	115	Devices, small, hydrocarbon gas powered, with release device
3150	115	Hydrocarbon gas refills for small devices, with release device
3151	171	Halogenated monomethyldiphenylmethanes, liquid
3151	171	Polyhalogenated biphenyls, liquid
3151	171	Polyhalogenated terphenyls, liquid
3152	171	Halogenated monomethyldiphenylmethanes, solid
3152	171	Polyhalogenated biphenyls, solid
3152	171	Polyhalogenated terphenyls, solid
3153	115	Perfluoro(methyl vinyl ether)
3154	115	Perfluoro(ethyl vinyl ether)
3155	154	Pentachlorophenol
3156	122	Compressed gas, oxidizing, n.o.s.
3157	122	Liquefied gas, oxidizing, n.o.s.
3158	120	Gas, refrigerated liquid, n.o.s.
3159	126	Refrigerant gas R-134a
3159	126	1,1,1,2-Tetrafluoroethane
3160	119	Liquefied gas, poisonous, flammable, n.o.s.

ID No.	Guide No.	Name of Material
3160	119	Liquefied gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone A)
3160	119	Liquefied gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone B)
3160	119	Liquefied gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone C)
3160	119	Liquefied gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone D)
3160	119	Liquefied gas, toxic, flammable, n.o.s.
3160	119	Liquefied gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone A)
3160	119	Liquefied gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone B)
3160	119	Liquefied gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone C)
3160	119	Liquefied gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone D)
3161	115	Liquefied gas, flammable, n.o.s.
3162	123	Liquefied gas, poisonous, n.o.s.
3162	123	Liquefied gas, poisonous, n.o.s. (Inhalation Hazard Zone A)
3162	123	Liquefied gas, poisonous, n.o.s. (Inhalation Hazard Zone B)
3162	123	Liquefied gas, poisonous, n.o.s. (Inhalation Hazard Zone C)
3162	123	Liquefied gas, poisonous, n.o.s. (Inhalation Hazard Zone D)
3162	123	Liquefied gas, toxic, n.o.s.
3162	123	Liquefied gas, toxic, n.o.s. (Inhalation Hazard Zone A)
3162	123	Liquefied gas, toxic, n.o.s. (Inhalation Hazard Zone B)
3162	123	Liquefied gas, toxic, n.o.s. (Inhalation Hazard Zone C)
3162	123	Liquefied gas, toxic, n.o.s. (Inhalation Hazard Zone D)
3163	126	Liquefied gas, n.o.s.
3164	126	Articles, pressurized, hydraulic (containing non-flammable gas)
3164	126	Articles, pressurized, pneumatic (containing non-flammable gas)
3165	131	Aircraft hydraulic power unit fuel tank
3166	115	Engine, fuel cell, flammable gas powered
3166	128	Engine, fuel cell, flammable liquid powered
3166	128	Engine, internal combustion
3166	115	Engines, internal combustion, flammable gas powered
3166	128	Engines, internal combustion, flammable liquid powered
3166	115	Vehicle, flammable gas powered
3166	128	Vehicle, flammable liquid powered
3166	115	Vehicle, fuel cell, flammable gas powered
3166	128	Vehicle, fuel cell, flammable liquid powered
3167	115	Gas sample, non-pressurized, flammable, n.o.s., not refrigerated liquid
3168	119	Gas sample, non-pressurized, poisonous, flammable, n.o.s., not refrigerated liquid
3168	119	Gas sample, non-pressurized, toxic, flammable, n.o.s., not refrigerated liquid

ID No.	Guide No.	Name of Material
3169	**123**	Gas sample, non-pressurized, poisonous, n.o.s., not refrigerated liquid
3169	**123**	Gas sample, non-pressurized, toxic, n.o.s., not refrigerated liquid
3170	**138**	Aluminum dross
3170	**138**	Aluminum remelting by-products
3170	**138**	Aluminum smelting by-products
3171	**154**	Battery-powered equipment (wet battery)
3171	**147**	Battery-powered equipment (with lithium ion batteries)
3171	**138**	Battery-powered equipment (with lithium metal batteries)
3171	**138**	Battery-powered equipment (with sodium batteries)
3171	**154**	Battery-powered vehicle (wet battery)
3171	**147**	Battery-powered vehicle (with lithium ion batteries)
3171	**138**	Battery-powered vehicle (with sodium batteries)
3171	**154**	Wheelchair, electric, with batteries
3172	**153**	Toxins, extracted from living sources, liquid, n.o.s.
3174	**135**	Titanium disulfide
3174	**135**	Titanium disulphide
3175	**133**	Solids containing flammable liquid, n.o.s.
3176	**133**	Flammable solid, organic, molten, n.o.s.
3178	**133**	Flammable solid, inorganic, n.o.s.
3178	**133**	Smokeless powder for small arms
3179	**134**	Flammable solid, poisonous, inorganic, n.o.s.
3179	**134**	Flammable solid, toxic, inorganic, n.o.s.
3180	**134**	Flammable solid, corrosive, inorganic, n.o.s.
3181	**133**	Metal salts of organic compounds, flammable, n.o.s.
3182	**170**	Metal hydrides, flammable, n.o.s.
3183	**135**	Self-heating liquid, organic, n.o.s.
3184	**136**	Self-heating liquid, poisonous, organic, n.o.s.
3184	**136**	Self-heating liquid, toxic, organic, n.o.s.
3185	**136**	Self-heating liquid, corrosive, organic, n.o.s.
3186	**135**	Self-heating liquid, inorganic, n.o.s.
3187	**136**	Self-heating liquid, poisonous, inorganic, n.o.s.
3187	**136**	Self-heating liquid, toxic, inorganic, n.o.s.
3188	**136**	Self-heating liquid, corrosive, inorganic, n.o.s.
3189	**135**	Metal powder, self-heating, n.o.s.
3190	**135**	Self-heating solid, inorganic, n.o.s.
3191	**136**	Self-heating solid, poisonous, inorganic, n.o.s.
3191	**136**	Self-heating solid, toxic, inorganic, n.o.s.
3192	**136**	Self-heating solid, corrosive, inorganic, n.o.s.
3194	**135**	Pyrophoric liquid, inorganic, n.o.s.
3200	**135**	Pyrophoric solid, inorganic, n.o.s.

ID No.	Guide No.	Name of Material
3205	135	Alkaline earth metal alcoholates, n.o.s.
3206	136	Alkali metal alcoholates, self-heating, corrosive, n.o.s.
3208	138	Metallic substance, water-reactive, n.o.s.
3209	138	Metallic substance, water-reactive, self-heating, n.o.s.
3210	140	Chlorates, inorganic, aqueous solution, n.o.s.
3211	140	Perchlorates, inorganic, aqueous solution, n.o.s.
3212	140	Hypochlorites, inorganic, n.o.s.
3213	140	Bromates, inorganic, aqueous solution, n.o.s.
3214	140	Permanganates, inorganic, aqueous solution, n.o.s.
3215	140	Persulfates, inorganic, n.o.s.
3215	140	Persulphates, inorganic, n.o.s.
3216	140	Persulfates, inorganic, aqueous solution, n.o.s.
3216	140	Persulphates, inorganic, aqueous solution, n.o.s.
3218	140	Nitrates, inorganic, aqueous solution, n.o.s.
3219	140	Nitrites, inorganic, aqueous solution, n.o.s.
3220	126	Pentafluoroethane
3220	126	Refrigerant gas R-125
3221	149	Self-reactive liquid type B
3222	149	Self-reactive solid type B
3223	149	Self-reactive liquid type C
3224	149	Self-reactive solid type C
3225	149	Self-reactive liquid type D
3226	149	Self-reactive solid type D
3227	149	Self-reactive liquid type E
3228	149	Self-reactive solid type E
3229	149	Self-reactive liquid type F
3230	149	Self-reactive solid type F
3231	150	Self-reactive liquid type B, temperature controlled
3232	150	Self-reactive solid type B, temperature controlled
3233	150	Self-reactive liquid type C, temperature controlled
3234	150	Self-reactive solid type C, temperature controlled
3235	150	Self-reactive liquid type D, temperature controlled
3236	150	Self-reactive solid type D, temperature controlled
3237	150	Self-reactive liquid type E, temperature controlled
3238	150	Self-reactive solid type E, temperature controlled
3239	150	Self-reactive liquid type F, temperature controlled
3240	150	Self-reactive solid type F, temperature controlled
3241	133	2-Bromo-2-nitropropane-1, 3-diol
3242	149	Azodicarbonamide
3243	151	Solids containing poisonous liquid, n.o.s.
3243	151	Solids containing toxic liquid, n.o.s.
3244	154	Solids containing corrosive liquid, n.o.s.
3245	171	Genetically modified micro-organisms
3245	171	Genetically modified organisms
3246	156	Methanesulfonyl chloride
3246	156	Methanesulphonyl chloride

ID No.	Guide No.	Name of Material
3247	140	Sodium peroxoborate, anhydrous
3248	131	Medicine, liquid, flammable, poisonous, n.o.s.
3248	131	Medicine, liquid, flammable, toxic, n.o.s.
3249	151	Medicine, solid, poisonous, n.o.s.
3249	151	Medicine, solid, toxic, n.o.s.
3250	153	Chloroacetic acid, molten
3251	133	Isosorbide-5-mononitrate
3252	115	Difluoromethane
3252	115	Refrigerant gas R-32
3253	154	Disodium trioxosilicate
3254	135	Tributylphosphane
3255	135	tert-Butyl hypochlorite
3256	128	Elevated temperature liquid, flammable, n.o.s., with flash point above 37.8°C (100°F), at or above its flash point
3256	128	Elevated temperature liquid, flammable, n.o.s., with flash point above 60°C (140°F), at or above its flash point
3257	171	Elevated temperature liquid, n.o.s., at or above 100°C (212°F), and below its flash point
3258	171	Elevated temperature solid, n.o.s., at or above 240°C (464°F)
3259	154	Amines, solid, corrosive, n.o.s.
3259	154	Polyamines, solid, corrosive, n.o.s.
3260	154	Corrosive solid, acidic, inorganic, n.o.s.
3261	154	Corrosive solid, acidic, organic, n.o.s.
3262	154	Corrosive solid, basic, inorganic, n.o.s.
3263	154	Corrosive solid, basic, organic, n.o.s.
3264	154	Corrosive liquid, acidic, inorganic, n.o.s.
3265	153	Corrosive liquid, acidic, organic, n.o.s.
3266	154	Corrosive liquid, basic, inorganic, n.o.s.
3267	153	Corrosive liquid, basic, organic, n.o.s.
3268	171	Air bag inflators
3268	171	Air bag modules
3268	171	Safety devices
3268	171	Seat-belt pre-tensioners
3269	128	Polyester resin kit, liquid base material
3270	133	Nitrocellulose membrane filters
3271	127	Ethers, n.o.s.
3272	127	Esters, n.o.s.
3273	131	Nitriles, flammable, poisonous, n.o.s.
3273	131	Nitriles, flammable, toxic, n.o.s.
3274	132	Alcoholates solution, n.o.s., in alcohol
3275	131	Nitriles, poisonous, flammable, n.o.s.
3275	131	Nitriles, toxic, flammable, n.o.s.
3276	151	Nitriles, liquid, poisonous, n.o.s.
3276	151	Nitriles, liquid, toxic, n.o.s.
3276	151	Nitriles, poisonous, liquid, n.o.s.
3276	151	Nitriles, toxic, liquid, n.o.s.
3277	154	Chloroformates, poisonous, corrosive, n.o.s.

ID No.	Guide No.	Name of Material
3277	154	Chloroformates, toxic, corrosive, n.o.s.
3278	151	Organophosphorus compound, liquid, poisonous, n.o.s.
3278	151	Organophosphorus compound, liquid, toxic, n.o.s.
3278	151	Organophosphorus compound, poisonous, liquid, n.o.s.
3278	151	Organophosphorus compound, toxic, liquid, n.o.s.
3279	131	Organophosphorus compound, poisonous, flammable, n.o.s.
3279	131	Organophosphorus compound, toxic, flammable, n.o.s.
3280	151	Organoarsenic compound, liquid, n.o.s.
3281	151	Metal carbonyls, liquid, n.o.s.
3282	151	Organometallic compound, liquid, poisonous, n.o.s.
3282	151	Organometallic compound, liquid, toxic, n.o.s.
3282	151	Organometallic compound, poisonous, liquid, n.o.s.
3282	151	Organometallic compound, toxic, liquid, n.o.s.
3283	151	Selenium compound, solid, n.o.s.
3284	151	Tellurium compound, n.o.s.
3285	151	Vanadium compound, n.o.s.
3286	131	Flammable liquid, poisonous, corrosive, n.o.s.
3286	131	Flammable liquid, toxic, corrosive, n.o.s.
3287	151	Poisonous liquid, inorganic, n.o.s.
3287	151	Toxic liquid, inorganic, n.o.s.
3288	151	Poisonous solid, inorganic, n.o.s.
3288	151	Toxic solid, inorganic, n.o.s.
3289	154	Poisonous liquid, corrosive, inorganic, n.o.s.
3289	154	Toxic liquid, corrosive, inorganic, n.o.s.
3290	154	Poisonous solid, corrosive, inorganic, n.o.s.
3290	154	Toxic solid, corrosive, inorganic, n.o.s.
3291	158	(Bio)Medical waste, n.o.s.
3291	158	Clinical waste, unspecified, n.o.s.
3291	158	Medical waste, n.o.s.
3291	158	Regulated medical waste, n.o.s.
3292	138	Batteries, containing Sodium
3292	138	Cells, containing Sodium
3292	138	Sodium, batteries containing
3293	152	Hydrazine, aqueous solution, with not more than 37% Hydrazine
3294	131	Hydrogen cyanide, solution in alcohol, with not more than 45% Hydrogen cyanide
3295	128	Hydrocarbons, liquid, n.o.s.
3296	126	Heptafluoropropane
3296	126	Refrigerant gas R-227
3297	126	Chlorotetrafluoroethane and Ethylene oxide mixture, with not more than 8.8% Ethylene oxide
3297	126	Ethylene oxide and Chlorotetrafluoroethane mixture, with not more than 8.8% Ethylene oxide
3298	126	Ethylene oxide and Pentafluoroethane mixture, with not more than 7.9% Ethylene oxide

ID No.	Guide No.	Name of Material
3298	**126**	Pentafluoroethane and Ethylene oxide mixture, with not more than 7.9% Ethylene oxide
3299	**126**	Ethylene oxide and Tetrafluoroethane mixture, with not more than 5.6% Ethylene oxide
3299	**126**	Tetrafluoroethane and Ethylene oxide mixture, with not more than 5.6% Ethylene oxide
3300	**119P**	Carbon dioxide and Ethylene oxide mixture, with more than 87% Ethylene oxide
3300	**119P**	Ethylene oxide and Carbon dioxide mixture, with more than 87% Ethylene oxide
3301	**136**	Corrosive liquid, self-heating, n.o.s.
3302	**152**	2-Dimethylaminoethyl acrylate
3303	**124**	Compressed gas, poisonous, oxidizing, n.o.s.
3303	**124**	Compressed gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone A)
3303	**124**	Compressed gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone B)
3303	**124**	Compressed gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone C)
3303	**124**	Compressed gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone D)
3303	**124**	Compressed gas, toxic, oxidizing, n.o.s.
3303	**124**	Compressed gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone A)
3303	**124**	Compressed gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone B)
3303	**124**	Compressed gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone C)
3303	**124**	Compressed gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone D)
3304	**125**	Compressed gas, poisonous, corrosive, n.o.s.
3304	**125**	Compressed gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone A)
3304	**125**	Compressed gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone B)
3304	**125**	Compressed gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone C)
3304	**125**	Compressed gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone D)
3304	**125**	Compressed gas, toxic, corrosive, n.o.s.
3304	**125**	Compressed gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone A)
3304	**125**	Compressed gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone B)
3304	**125**	Compressed gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone C)
3304	**125**	Compressed gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone D)
3305	**119**	Compressed gas, poisonous, flammable, corrosive, n.o.s.
3305	**119**	Compressed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)
3305	**119**	Compressed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)

ID No.	Guide No.	Name of Material
3305	119	Compressed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone C)
3305	119	Compressed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone D)
3305	119	Compressed gas, toxic, flammable, corrosive, n.o.s.
3305	119	Compressed gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)
3305	119	Compressed gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)
3305	119	Compressed gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone C)
3305	119	Compressed gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone D)
3306	124	Compressed gas, poisonous, oxidizing, corrosive, n.o.s.
3306	124	Compressed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone A)
3306	124	Compressed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone B)
3306	124	Compressed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone C)
3306	124	Compressed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone D)
3306	124	Compressed gas, toxic, oxidizing, corrosive, n.o.s.
3306	124	Compressed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone A)
3306	124	Compressed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone B)
3306	124	Compressed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone C)
3306	124	Compressed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone D)
3307	124	Liquefied gas, poisonous, oxidizing, n.o.s.
3307	124	Liquefied gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone A)
3307	124	Liquefied gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone B)
3307	124	Liquefied gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone C)
3307	124	Liquefied gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone D)
3307	124	Liquefied gas, toxic, oxidizing, n.o.s.
3307	124	Liquefied gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone A)
3307	124	Liquefied gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone B)
3307	124	Liquefied gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone C)
3307	124	Liquefied gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone D)
3308	125	Liquefied gas, poisonous, corrosive, n.o.s.
3308	125	Liquefied gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone A)
3308	125	Liquefied gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone B)

ID No.	Guide No.	Name of Material
3308	125	Liquefied gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone C)
3308	125	Liquefied gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone D)
3308	125	Liquefied gas, toxic, corrosive, n.o.s.
3308	125	Liquefied gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone A)
3308	125	Liquefied gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone B)
3308	125	Liquefied gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone C)
3308	125	Liquefied gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone D)
3309	119	Liquefied gas, poisonous, flammable, corrosive, n.o.s.
3309	119	Liquefied gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)
3309	119	Liquefied gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)
3309	119	Liquefied gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone C)
3309	119	Liquefied gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone D)
3309	119	Liquefied gas, toxic, flammable, corrosive, n.o.s.
3309	119	Liquefied gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)
3309	119	Liquefied gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)
3309	119	Liquefied gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone C)
3309	119	Liquefied gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone D)
3310	124	Liquefied gas, poisonous, oxidizing, corrosive, n.o.s.
3310	124	Liquefied gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone A)
3310	124	Liquefied gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone B)
3310	124	Liquefied gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone C)
3310	124	Liquefied gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone D)
3310	124	Liquefied gas, toxic, oxidizing, corrosive, n.o.s.
3310	124	Liquefied gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone A)
3310	124	Liquefied gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone B)
3310	124	Liquefied gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone C)
3310	124	Liquefied gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone D)
3311	122	Gas, refrigerated liquid, oxidizing, n.o.s.
3312	115	Gas, refrigerated liquid, flammable, n.o.s.
3313	135	Organic pigments, self-heating
3314	171	Plastic molding compound
3314	171	Plastics moulding compound

ID No.	Guide No.	Name of Material
3315	**151**	Chemical sample, poisonous
3315	**151**	Chemical sample, toxic
3316	**171**	Chemical kit
3316	**171**	First aid kit
3317	**113**	2-Amino-4,6-dinitrophenol, wetted with not less than 20% water
3318	**125**	Ammonia solution, with more than 50% Ammonia
3319	**113**	Nitroglycerin mixture, desensitized, solid, n.o.s., with more than 2% but not more than 10% Nitroglycerin
3320	**157**	Sodium borohydride and Sodium hydroxide solution, with not more than 12% Sodium borohydride and not more than 40% Sodium hydroxide
3321	**162**	Radioactive material, low specific activity (LSA-II), non fissile or fissile-excepted
3322	**162**	Radioactive material, low specific activity (LSA-III), non fissile or fissile-excepted
3323	**163**	Radioactive material, Type C package, non fissile or fissile excepted
3324	**165**	Radioactive material, low specific activity (LSA-II), fissile
3325	**165**	Radioactive material, low specific activity (LSA-III), fissile
3326	**165**	Radioactive material, surface contaminated objects (SCO-I), fissile
3326	**165**	Radioactive material, surface contaminated objects (SCO-II), fissile
3327	**165**	Radioactive material, Type A package, fissile, non-special form
3328	**165**	Radioactive material, Type B(U) package, fissile
3329	**165**	Radioactive material, Type B(M) package, fissile
3330	**165**	Radioactive material, Type C package, fissile
3331	**165**	Radioactive material, transported under special arrangement, fissile
3332	**164**	Radioactive material, Type A package, special form, non fissile or fissile-excepted
3333	**165**	Radioactive material, Type A package, special form, fissile
3334	**171**	Aviation regulated liquid, n.o.s.
3334	**171**	Self-defense spray, non-pressurized
3335	**171**	Aviation regulated solid, n.o.s.
3336	**130**	Mercaptan mixture, liquid, flammable, n.o.s.
3336	**130**	Mercaptans, liquid, flammable, n.o.s.
3337	**126**	Refrigerant gas R-404A
3338	**126**	Refrigerant gas R-407A
3339	**126**	Refrigerant gas R-407B
3340	**126**	Refrigerant gas R-407C
3341	**135**	Thiourea dioxide
3342	**135**	Xanthates
3343	**113**	Nitroglycerin mixture, desensitized, liquid, flammable, n.o.s., with not more than 30% Nitroglycerin
3344	**113**	Pentaerythrite tetranitrate mixture, desensitized, solid, n.o.s., with more than 10% but not more than 20% PETN

ID No.	Guide No.	Name of Material
3344	113	Pentaerythritol tetranitrate mixture, desensitized, solid, n.o.s., with more than 10% but not more than 20% PETN
3344	113	PETN mixture, desensitized, solid, n.o.s., with more than 10% but not more than 20% PETN
3345	153	Phenoxyacetic acid derivative pesticide, solid, poisonous
3345	153	Phenoxyacetic acid derivative pesticide, solid, toxic
3346	131	Phenoxyacetic acid derivative pesticide, liquid, flammable, poisonous
3346	131	Phenoxyacetic acid derivative pesticide, liquid, flammable, toxic
3347	131	Phenoxyacetic acid derivative pesticide, liquid, poisonous, flammable
3347	131	Phenoxyacetic acid derivative pesticide, liquid, toxic, flammable
3348	153	Phenoxyacetic acid derivative pesticide, liquid, poisonous
3348	153	Phenoxyacetic acid derivative pesticide, liquid, toxic
3349	151	Pyrethroid pesticide, solid, poisonous
3349	151	Pyrethroid pesticide, solid, toxic
3350	131	Pyrethroid pesticide, liquid, flammable, poisonous
3350	131	Pyrethroid pesticide, liquid, flammable, toxic
3351	131	Pyrethroid pesticide, liquid, poisonous, flammable
3351	131	Pyrethroid pesticide, liquid, toxic, flammable
3352	151	Pyrethroid pesticide, liquid, poisonous
3352	151	Pyrethroid pesticide, liquid, toxic
3354	115	Insecticide gas, flammable, n.o.s.
3355	119	Insecticide gas, poisonous, flammable, n.o.s.
3355	119	Insecticide gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone A)
3355	119	Insecticide gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone B)
3355	119	Insecticide gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone C)
3355	119	Insecticide gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone D)
3355	119	Insecticide gas, toxic, flammable, n.o.s.
3355	119	Insecticide gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone A)
3355	119	Insecticide gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone B)
3355	119	Insecticide gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone C)
3355	119	Insecticide gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone D)
3356	140	Oxygen generator, chemical
3356	140	Oxygen generator, chemical, spent
3357	113	Nitroglycerin mixture, desensitized, liquid, n.o.s., with not more than 30% Nitroglycerin
3358	115	Refrigerating machines, containing flammable, non-poisonous, liquefied gas

ID No.	Guide No.	Name of Material
3358	115	Refrigerating machines, containing flammable, non-toxic, liquefied gas
3359	171	Fumigated cargo transport unit
3360	133	Fibers, vegetable, dry
3360	133	Fibres, vegetable, dry
3361	156	Chlorosilanes, poisonous, corrosive, n.o.s.
3361	156	Chlorosilanes, toxic, corrosive, n.o.s.
3362	155	Chlorosilanes, poisonous, corrosive, flammable, n.o.s.
3362	155	Chlorosilanes, toxic, corrosive, flammable, n.o.s.
3363	171	Dangerous goods in apparatus
3363	171	Dangerous goods in articles
3363	171	Dangerous goods in machinery
3364	113	Picric acid, wetted with not less than 10% water
3364	113	Trinitrophenol, wetted with not less than 10% water
3365	113	Picryl chloride, wetted with not less than 10% water
3365	113	Trinitrochlorobenzene, wetted with not less than 10% water
3366	113	TNT, wetted with not less than 10% water
3366	113	Trinitrotoluene, wetted with not less than 10% water
3367	113	Trinitrobenzene, wetted with not less than 10% water
3368	113	Trinitrobenzoic acid, wetted with not less than 10% water
3369	113	Sodium dinitro-o-cresolate, wetted with not less than 10% water
3370	113	Urea nitrate, wetted with not less than 10% water
3371	129	2-Methylbutanal
3373	158	Biological substance, category B
3374	116	Acetylene, solvent free
3375	140	Ammonium nitrate emulsion
3375	140	Ammonium nitrate gel
3375	140	Ammonium nitrate suspension
3376	113	4-Nitrophenylhydrazine, with not less than 30% water
3377	140	Sodium perborate monohydrate
3378	140	Sodium carbonate peroxyhydrate
3379	113	Desensitized explosive, liquid, n.o.s.
3380	113	Desensitized explosive, solid, n.o.s.
3381	151	Poisonous by inhalation liquid, n.o.s. (Inhalation Hazard Zone A)
3381	151	Toxic by inhalation liquid, n.o.s. (Inhalation Hazard Zone A)
3382	151	Poisonous by inhalation liquid, n.o.s. (Inhalation Hazard Zone B)
3382	151	Toxic by inhalation liquid, n.o.s. (Inhalation Hazard Zone B)
3383	131	Poisonous by inhalation liquid, flammable, n.o.s. (Inhalation Hazard Zone A)
3383	131	Toxic by inhalation liquid, flammable, n.o.s. (Inhalation Hazard Zone A)
3384	131	Poisonous by inhalation liquid, flammable, n.o.s. (Inhalation Hazard Zone B)
3384	131	Toxic by inhalation liquid, flammable, n.o.s. (Inhalation Hazard Zone B)
3385	139	Poisonous by inhalation liquid, water-reactive, n.o.s. (Inhalation Hazard Zone A)

ID No.	Guide No.	Name of Material
3385	139	Toxic by inhalation liquid, water-reactive, n.o.s. (Inhalation Hazard Zone A)
3386	139	Poisonous by inhalation liquid, water-reactive, n.o.s. (Inhalation Hazard Zone B)
3386	139	Toxic by inhalation liquid, water-reactive, n.o.s. (Inhalation Hazard Zone B)
3387	142	Poisonous by inhalation liquid, oxidizing, n.o.s. (Inhalation Hazard Zone A)
3387	142	Toxic by inhalation liquid, oxidizing, n.o.s. (Inhalation Hazard Zone A)
3388	142	Poisonous by inhalation liquid, oxidizing, n.o.s. (Inhalation Hazard Zone B)
3388	142	Toxic by inhalation liquid, oxidizing, n.o.s. (Inhalation Hazard Zone B)
3389	154	Poisonous by inhalation liquid, corrosive, n.o.s. (Inhalation Hazard Zone A)
3389	154	Toxic by inhalation liquid, corrosive, n.o.s. (Inhalation Hazard Zone A)
3390	154	Poisonous by inhalation liquid, corrosive, n.o.s. (Inhalation Hazard Zone B)
3390	154	Toxic by inhalation liquid, corrosive, n.o.s. (Inhalation Hazard Zone B)
3391	135	Organometallic substance, solid, pyrophoric
3392	135	Organometallic substance, liquid, pyrophoric
3393	135	Organometallic substance, solid, pyrophoric, water-reactive
3394	135	Organometallic substance, liquid, pyrophoric, water-reactive
3395	135	Organometallic substance, solid, water-reactive
3396	138	Organometallic substance, solid, water-reactive, flammable
3397	138	Organometallic substance, solid, water-reactive, self-heating
3398	135	Organometallic substance, liquid, water-reactive
3399	138	Organometallic substance, liquid, water-reactive, flammable
3400	138	Organometallic substance, solid, self-heating
3401	138	Alkali metal amalgam, solid
3402	138	Alkaline earth metal amalgam, solid
3403	138	Potassium, metal alloys, solid
3404	138	Potassium sodium alloys, solid
3404	138	Sodium potassium alloys, solid
3405	141	Barium chlorate, solution
3406	141	Barium perchlorate, solution
3407	140	Chlorate and Magnesium chloride mixture, solution
3407	140	Magnesium chloride and Chlorate mixture, solution
3408	141	Lead perchlorate, solution
3409	152	Chloronitrobenzenes, liquid
3410	153	4-Chloro-o-toluidine hydrochloride, solution
3411	153	beta-Naphthylamine, solution
3411	153	Naphthylamine (beta), solution
3412	153	Formic acid, with not less than 5% but less than 10% acid
3412	153	Formic acid, with not less than 10% but not more than 85% acid

ID No.	Guide No.	Name of Material
3413	157	Potassium cyanide, solution
3414	157	Sodium cyanide, solution
3415	154	Sodium fluoride, solution
3416	153	Chloroacetophenone, liquid
3417	152	Xylyl bromide, solid
3418	151	2,4-Toluenediamine, solution
3418	151	2,4-Toluylenediamine, solution
3419	157	Boron trifluoride acetic acid complex, solid
3420	157	Boron trifluoride propionic acid complex, solid
3421	154	Potassium hydrogen difluoride, solution
3422	154	Potassium fluoride, solution
3423	153	Tetramethylammonium hydroxide, solid
3424	141	Ammonium dinitro-o-cresolate, solution
3425	156	Bromoacetic acid, solid
3426	153P	Acrylamide, solution
3427	153	Chlorobenzyl chlorides, solid
3428	156	3-Chloro-4-methylphenyl isocyanate, solid
3429	153	Chlorotoluidines, liquid
3430	153	Xylenols, liquid
3431	152	Nitrobenzotrifluorides, solid
3432	171	Polychlorinated biphenyls, solid
3434	153	Nitrocresols, liquid
3436	151	Hexafluoroacetone hydrate, solid
3437	152	Chlorocresols, solid
3438	153	alpha-Methylbenzyl alcohol, solid
3438	153	Methylbenzyl (alpha) alcohol, solid
3439	151	Nitriles, poisonous, solid, n.o.s.
3439	151	Nitriles, solid, poisonous, n.o.s.
3439	151	Nitriles, solid, toxic, n.o.s.
3439	151	Nitriles, toxic, solid, n.o.s.
3440	151	Selenium compound, liquid, n.o.s.
3441	153	Chlorodinitrobenzenes, solid
3442	153	Dichloroanilines, solid
3443	152	Dinitrobenzenes, solid
3444	151	Nicotine hydrochloride, solid
3445	151	Nicotine sulfate, solid
3445	151	Nicotine sulphate, solid
3446	152	Nitrotoluenes, solid
3447	152	Nitroxylenes, solid
3448	159	Tear gas substance, solid, n.o.s.
3449	159	Bromobenzyl cyanides, solid
3450	151	Diphenylchloroarsine, solid
3451	153	Toluidines, solid
3452	153	Xylidines, solid
3453	154	Phosphoric acid, solid
3454	152	Dinitrotoluenes, solid
3455	153	Cresols, solid
3456	157	Nitrosylsulfuric acid, solid
3456	157	Nitrosylsulphuric acid, solid
3457	152	Chloronitrotoluenes, solid
3458	152	Nitroanisoles, solid
3459	152	Nitrobromobenzenes, solid
3460	153	N-Ethylbenzyltoluidines, solid
3462	153	Toxins, extracted from living sources, solid, n.o.s.
3463	153	Propionic acid, with not less than 90% acid

ID No.	Guide No.	Name of Material
3464	151	Organophosphorus compound, poisonous, solid, n.o.s.
3464	151	Organophosphorus compound, solid, poisonous, n.o.s.
3464	151	Organophosphorus compound, solid, toxic, n.o.s.
3464	151	Organophosphorus compound, toxic, solid, n.o.s.
3465	151	Organoarsenic compound, solid, n.o.s.
3466	151	Metal carbonyls, solid, n.o.s.
3467	151	Organometallic compound, poisonous, solid, n.o.s.
3467	151	Organometallic compound, solid, poisonous, n.o.s.
3467	151	Organometallic compound, solid, toxic, n.o.s.
3467	151	Organometallic compound, toxic, solid, n.o.s.
3468	115	Hydrogen in a metal hydride storage system
3468	115	Hydrogen in a metal hydride storage system contained in equipment
3468	115	Hydrogen in a metal hydride storage system packed with equipment
3469	132	Paint, flammable, corrosive
3469	132	Paint related material, flammable, corrosive
3470	132	Paint, corrosive, flammable
3470	132	Paint related material, corrosive, flammable
3471	154	Hydrogendifluorides, solution, n.o.s.
3472	153	Crotonic acid, liquid
3473	128	Fuel cell cartridges, containing flammable liquids
3473	128	Fuel cell cartridges contained in equipment, containing flammable liquids
3473	128	Fuel cell cartridges packed with equipment, containing flammable liquids
3474	113	1-Hydroxybenzotriazole, anhydrous, wetted with not less than 20% water
3474	113	1-Hydroxybenzotriazole, monohydrate
3475	127	Ethanol and gasoline mixture, with more than 10% ethanol
3475	127	Ethanol and motor spirit mixture, with more than 10% ethanol
3475	127	Ethanol and petrol mixture, with more than 10% ethanol
3475	127	Gasoline and ethanol mixture, with more than 10% ethanol
3475	127	Motor spirit and ethanol mixture, with more than 10% ethanol
3475	127	Petrol and ethanol mixture, with more than 10% ethanol
3476	138	Fuel cell cartridges, containing water-reactive substances
3476	138	Fuel cell cartridges contained in equipment, containing water-reactive substances
3476	138	Fuel cell cartridges packed with equipment, containing water-reactive substances
3477	153	Fuel cell cartridges, containing corrosive substances
3477	153	Fuel cell cartridges contained in equipment, containing corrosive substances
3477	153	Fuel cell cartridges packed with equipment, containing corrosive substances

ID No.	Guide No.	Name of Material
3478	115	Fuel cell cartridges, containing liquefied flammable gas
3478	115	Fuel cell cartridges contained in equipment, containing liquefied flammable gas
3478	115	Fuel cell cartridges packed with equipment, containing liquefied flammable gas
3479	115	Fuel cell cartridges, containing hydrogen in metal hydride
3479	115	Fuel cell cartridges contained in equipment, containing hydrogen in metal hydride
3479	115	Fuel cell cartridges packed with equipment, containing hydrogen in metal hydride
3480	147	Lithium ion batteries (including lithium ion polymer batteries)
3481	147	Lithium ion batteries contained in equipment (including lithium ion polymer batteries)
3481	147	Lithium ion batteries packed with equipment (including lithium ion polymer batteries)
3482	138	Alkali metal dispersion, flammable
3482	138	Alkaline earth metal dispersion, flammable
3483	131	Motor fuel anti-knock mixture, flammable
3484	132	Hydrazine aqueous solution, flammable, with more than 37% hydrazine, by mass
3485	140	Calcium hypochlorite, dry, corrosive, with more than 39% available chlorine (8.8% available oxygen)
3485	140	Calcium hypochlorite mixture, dry, corrosive, with more than 39% available chlorine (8.8% available oxygen)
3486	140	Calcium hypochlorite mixture, dry, corrosive, with more than 10% but not more than 39% available chlorine
3487	140	Calcium hypochlorite, hydrated, corrosive, with not less than 5.5% but not more than 16% water
3487	140	Calcium hypochlorite, hydrated mixture, corrosive, with not less than 5.5% but not more than 16% water
3488	131	Poisonous by inhalation liquid, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)
3488	131	Toxic by inhalation liquid, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)
3489	131	Poisonous by inhalation liquid, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)
3489	131	Toxic by inhalation liquid, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)
3490	155	Poisonous by inhalation liquid, water-reactive, flammable, n.o.s. (Inhalation Hazard Zone A)
3490	155	Toxic by inhalation liquid, water-reactive, flammable, n.o.s. (Inhalation Hazard Zone A)
3491	155	Poisonous by inhalation liquid, water-reactive, flammable, n.o.s. (Inhalation Hazard Zone B)
3491	155	Toxic by inhalation liquid, water-reactive, flammable, n.o.s. (Inhalation Hazard Zone B)
3492	131	Poisonous by inhalation liquid, corrosive, flammable, n.o.s. (Inhalation Hazard Zone A)
3492	131	Toxic by inhalation liquid, corrosive, flammable, n.o.s. (Inhalation Hazard Zone A)

ID No.	Guide No.	Name of Material
3493	131	Poisonous by inhalation liquid, corrosive, flammable, n.o.s. (Inhalation Hazard Zone B)
3493	131	Toxic by inhalation liquid, corrosive, flammable, n.o.s. (Inhalation Hazard Zone B)
3494	131	Petroleum sour crude oil, flammable, poisonous
3494	131	Petroleum sour crude oil, flammable, toxic
3495	154	Iodine
3496	171	Batteries, nickel-metal hydride
3497	133	Krill meal
3498	157	Iodine monochloride, liquid
3499	171	Capacitor, electric double layer
3500	126	Chemical under pressure, n.o.s.
3501	115	Chemical under pressure, flammable, n.o.s.
3502	123	Chemical under pressure, poisonous, n.o.s.
3502	123	Chemical under pressure, toxic, n.o.s.
3503	125	Chemical under pressure, corrosive, n.o.s.
3504	119	Chemical under pressure, flammable, poisonous, n.o.s.
3504	119	Chemical under pressure, flammable, toxic, n.o.s.
3505	118	Chemical under pressure, flammable, corrosive, n.o.s.
3506	172	Mercury contained in manufactured articles
3507	166	Uranium hexafluoride, radioactive material, excepted package, less than 0.1 kg per package, non-fissile or fissile-excepted
3508	171	Capacitor, asymmetric
3509	171	Packagings discarded, empty, uncleaned
3510	174	Adsorbed gas, flammable, n.o.s.
3511	174	Adsorbed gas, n.o.s.
3512	173	Adsorbed gas, poisonous, n.o.s.
3512	173	Adsorbed gas, poisonous, n.o.s. (Inhalation hazard zone A)
3512	173	Adsorbed gas, poisonous, n.o.s. (Inhalation hazard zone B)
3512	173	Adsorbed gas, poisonous, n.o.s. (Inhalation hazard zone C)
3512	173	Adsorbed gas, poisonous, n.o.s. (Inhalation hazard zone D)
3512	173	Adsorbed gas, toxic, n.o.s.
3512	173	Adsorbed gas, toxic, n.o.s. (Inhalation hazard zone A)
3512	173	Adsorbed gas, toxic, n.o.s. (Inhalation hazard zone B)
3512	173	Adsorbed gas, toxic, n.o.s. (Inhalation hazard zone C)
3512	173	Adsorbed gas, toxic, n.o.s. (Inhalation hazard zone D)
3513	174	Adsorbed gas, oxidizing, n.o.s.
3514	173	Adsorbed gas, poisonous, flammable, n.o.s.
3514	173	Adsorbed gas, poisonous, flammable, n.o.s. (Inhalation hazard zone A)
3514	173	Adsorbed gas, poisonous, flammable, n.o.s. (Inhalation hazard zone B)
3514	173	Adsorbed gas, poisonous, flammable, n.o.s. (Inhalation hazard zone C)
3514	173	Adsorbed gas, poisonous, flammable, n.o.s. (Inhalation hazard zone D)
3514	173	Adsorbed gas, toxic, flammable, n.o.s.

ID No.	Guide No.	Name of Material
3514	173	Adsorbed gas, toxic, flammable, n.o.s. (Inhalation hazard zone A)
3514	173	Adsorbed gas, toxic, flammable, n.o.s. (Inhalation hazard zone B)
3514	173	Adsorbed gas, toxic, flammable, n.o.s. (Inhalation hazard zone C)
3514	173	Adsorbed gas, toxic, flammable, n.o.s. (Inhalation hazard zone D)
3515	173	Adsorbed gas, poisonous, oxidizing, n.o.s.
3515	173	Adsorbed gas, poisonous, oxidizing, n.o.s. (Inhalation hazard zone A)
3515	173	Adsorbed gas, poisonous, oxidizing, n.o.s. (Inhalation hazard zone B)
3515	173	Adsorbed gas, poisonous, oxidizing, n.o.s. (Inhalation hazard zone C)
3515	173	Adsorbed gas, poisonous, oxidizing, n.o.s. (Inhalation hazard zone D)
3515	173	Adsorbed gas, toxic, oxidizing, n.o.s.
3515	173	Adsorbed gas, toxic, oxidizing, n.o.s. (Inhalation hazard zone A)
3515	173	Adsorbed gas, toxic, oxidizing, n.o.s. (Inhalation hazard zone B)
3515	173	Adsorbed gas, toxic, oxidizing, n.o.s. (Inhalation hazard zone C)
3515	173	Adsorbed gas, toxic, oxidizing, n.o.s. (Inhalation hazard zone D)
3516	173	Adsorbed gas, poisonous, corrosive, n.o.s.
3516	173	Adsorbed gas, poisonous, corrosive, n.o.s. (Inhalation hazard zone A)
3516	173	Adsorbed gas, poisonous, corrosive, n.o.s. (Inhalation hazard zone B)
3516	173	Adsorbed gas, poisonous, corrosive, n.o.s. (Inhalation hazard zone C)
3516	173	Adsorbed gas, poisonous, corrosive, n.o.s. (Inhalation hazard zone D)
3516	173	Adsorbed gas, toxic, corrosive, n.o.s.
3516	173	Adsorbed gas, toxic, corrosive, n.o.s. (Inhalation hazard zone A)
3516	173	Adsorbed gas, toxic, corrosive, n.o.s. (Inhalation hazard zone B)
3516	173	Adsorbed gas, toxic, corrosive, n.o.s. (Inhalation hazard zone C)
3516	173	Adsorbed gas, toxic, corrosive, n.o.s. (Inhalation hazard zone D)
3517	173	Adsorbed gas, poisonous, flammable, corrosive, n.o.s.
3517	173	Adsorbed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation hazard zone A)
3517	173	Adsorbed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation hazard zone B)
3517	173	Adsorbed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation hazard zone C)
3517	173	Adsorbed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation hazard zone D)
3517	173	Adsorbed gas, toxic, flammable, corrosive, n.o.s.

ID No.	Guide No.	Name of Material
3517	173	Adsorbed gas, toxic, flammable, corrosive, n.o.s. (Inhalation hazard zone A)
3517	173	Adsorbed gas, toxic, flammable, corrosive, n.o.s. (Inhalation hazard zone B)
3517	173	Adsorbed gas, toxic, flammable, corrosive, n.o.s. (Inhalation hazard zone C)
3517	173	Adsorbed gas, toxic, flammable, corrosive, n.o.s. (Inhalation hazard zone D)
3518	173	Adsorbed gas, poisonous, oxidizing, corrosive, n.o.s.
3518	173	Adsorbed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation hazard zone A)
3518	173	Adsorbed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation hazard zone B)
3518	173	Adsorbed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation hazard zone C)
3518	173	Adsorbed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation hazard zone D)
3518	173	Adsorbed gas, toxic, oxidizing, corrosive, n.o.s.
3518	173	Adsorbed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation hazard zone A)
3518	173	Adsorbed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation hazard zone B)
3518	173	Adsorbed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation hazard zone C)
3518	173	Adsorbed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation hazard zone D)
3519	173	Boron trifluoride, adsorbed
3520	173	Chlorine, adsorbed
3521	173	Silicon tetrafluoride, adsorbed
3522	173	Arsine, adsorbed
3523	173	Germane, adsorbed
3524	173	Phosphorus pentafluoride, adsorbed
3525	173	Phosphine, adsorbed
3526	173	Hydrogen selenide, adsorbed
3527	128P	Polyester resin kit, solid base material
3528	128	Engine, fuel cell, flammable liquid powered
3528	128	Engine, internal combustion, flammable liquid powered
3528	128	Machinery, fuel cell, flammable liquid powered
3528	128	Machinery, internal combustion, flammable liquid powered
3529	115	Engine, fuel cell, flammable gas powered
3529	115	Engine, internal combustion, flammable gas powered
3529	115	Machinery, fuel cell, flammable gas powered
3529	115	Machinery, internal combustion, flammable gas powered
3530	171	Engine, internal combustion
3530	171	Machinery, internal combustion
3531	149P	Polymerizing substance, solid, stabilized, n.o.s.
3532	149P	Polymerizing substance, liquid, stabilized, n.o.s.
3533	150P	Polymerizing substance, solid, temperature controlled, n.o.s.
3534	150P	Polymerizing substance, liquid, temperature controlled, n.o.s.
3535	134	Toxic solid, flammable, inorganic, n.o.s.

ID No.	Guide No.	Name of Material
3536	**147**	Lithium batteries installed in cargo transport unit (lithium ion batteries)
3536	**138**	Lithium batteries installed in cargo transport unit (lithium metal batteries)
3537	**115**	Articles containing flammable gas, n.o.s.
3538	**120**	Articles containing non-flammable, non-toxic gas, n.o.s.
3539	**123**	Articles containing toxic gas, n.o.s.
3540	**127**	Articles containing flammable liquid, n.o.s.
3541	**133**	Articles containing flammable solid, n.o.s.
3542	**135**	Articles containing a substance liable to spontaneous combustion, n.o.s.
3543	**138**	Articles containing a substance which emits flammable gas in contact with water, n.o.s.
3544	**140**	Articles containing oxidizing substance, n.o.s.
3545	**145**	Articles containing organic peroxide, n.o.s.
3546	**151**	Articles containing toxic substance, n.o.s.
3547	**154**	Articles containing corrosive substance, n.o.s.
3548	**171**	Articles containing miscellaneous dangerous goods, n.o.s.
3549	**158**	Medical waste, category A, affecting humans, solid
3549	**158**	Medical waste, category A, affecting animals only, solid
8000	**171**	Consumer commodity
9035	**123**	Gas identification set
9191	**143**	Chlorine dioxide, hydrate, frozen
9202	**168**	Carbon monoxide, refrigerated liquid (cryogenic liquid)
9206	**137**	Methyl phosphonic dichloride
9260	**169**	Aluminum, molten
9263	**156**	Chloropivaloyl chloride
9264	**151**	3,5-Dichloro-2,4,6-trifluoropyridine
9269	**132**	Trimethoxysilane

NOTES

INTRODUCTION TO BLUE PAGES

For entries highlighted in green follow these steps:

- **IF THERE IS NO FIRE**:
  - Go directly to **Table 1** (green-bordered pages)
  - Look up the ID number and name of material
  - Identify initial isolation and protective action distances
  - Also consult the appropriate Orange Guide

- **IF A FIRE IS INVOLVED**:
  - Use the appropriate Orange Guide for **EVACUATION** distances
  - Also protect in downwind direction according to Table 1 for residual material release

Note 1: If the name in **Table 1** is shown with **(when spilled in water)**, these materials produce large amounts of Toxic Inhalation Hazard (TIH) (PIH in the US) gases when spilled in water. Some Water Reactive materials are also TIH materials themselves (e.g., UN1746 (Bromine trifluoride), UN1836 (Thionyl chloride)). In these instances, two entries are provided in **Table 1** for land-based and water-based spills. If a water-reactive material only has one entry in Table 1 for **(when spilled in water)** and the product is NOT spilled in water, Table 1 and Table 2 do not apply. You will find safe distances in the appropriate orange-bordered guide.

Note 2: **Explosives** are not individually listed by their name because in an emergency situation, the response will be based only on the division of the explosive, not on the individual explosive.

For divisions 1.1, 1.2, 1.3 and 1.5, refer to GUIDE 112.

For divisions 1.4 and 1.6, refer to GUIDE 114.

Note 3: Chemical warfare agents do not have an assigned ID number because they are not commercially transported. In an emergency situation, the assigned orange guide will provide guidance for the initial response. Also consult “Criminal or Terrorist Use of Chemical, Biological and Radiological Agents”, pp. 368 to 372.

Name of Material	Guide No.	ID No.
AC	117	——
Acetal	127	1088
Acetaldehyde	129P	1089
Acetaldehyde ammonia	171	1841
Acetaldehyde oxime	129	2332
Acetic acid, glacial	132	2789
Acetic acid, solution, more than 10% but not more than 80% acid	153	2790
Acetic acid, solution, more than 80% acid	132	2789
Acetic anhydride	137	1715
Acetone	127	1090
Acetone cyanohydrin, stabilized	155	1541
Acetone oils	127	1091
Acetonitrile	127	1648
Acetyl bromide	156	1716
Acetyl chloride	155	1717
Acetylene, dissolved	116	1001
Acetylene, Ethylene and Propylene in mixture, refrigerated liquid containing at least 71.5% Ethylene with not more than 22.5% Acetylene and not more than 6% Propylene	115	3138
Acetylene, solvent free	116	3374
Acetylene tetrabromide	159	2504
Acetyl iodide	156	1898
Acetyl methyl carbinol	127	2621
Acid, sludge	153	1906
Acid butyl phosphate	153	1718
Acridine	153	2713
Acrolein, stabilized	131P	1092
Acrolein dimer, stabilized	129P	2607
Acrylamide, solid	153P	2074
Acrylamide, solution	153P	3426
Acrylic acid, stabilized	132P	2218
Acrylonitrile, stabilized	131P	1093
Adamsite	154	——
Adhesives (flammable)	128	1133
Adiponitrile	153	2205
Adsorbed gas, flammable, n.o.s.	174	3510
Adsorbed gas, n.o.s.	174	3511
Adsorbed gas, oxidizing, n.o.s.	174	3513
Adsorbed gas, poisonous, corrosive, n.o.s.	173	3516
Adsorbed gas, poisonous, corrosive, n.o.s. (Inhalation hazard zone A)	173	3516
Adsorbed gas, poisonous, corrosive, n.o.s. (Inhalation hazard zone B)	173	3516
Adsorbed gas, poisonous, corrosive, n.o.s. (Inhalation hazard zone C)	173	3516
Adsorbed gas, poisonous, corrosive, n.o.s. (Inhalation hazard zone D)	173	3516
Adsorbed gas, poisonous, flammable, corrosive, n.o.s.	173	3517
Adsorbed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation hazard zone A)	173	3517
Adsorbed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation hazard zone B)	173	3517
Adsorbed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation hazard zone C)	173	3517
Adsorbed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation hazard zone D)	173	3517

Name of Material	Guide No.	ID No.
Adsorbed gas, poisonous, flammable, n.o.s.	173	3514
Adsorbed gas, poisonous, flammable, n.o.s. (Inhalation hazard zone A)	173	3514
Adsorbed gas, poisonous, flammable, n.o.s. (Inhalation hazard zone B)	173	3514
Adsorbed gas, poisonous, flammable, n.o.s. (Inhalation hazard zone C)	173	3514
Adsorbed gas, poisonous, flammable, n.o.s. (Inhalation hazard zone D)	173	3514
Adsorbed gas, poisonous, n.o.s.	173	3512
Adsorbed gas, poisonous, n.o.s. (Inhalation hazard zone A)	173	3512
Adsorbed gas, poisonous, n.o.s. (Inhalation hazard zone B)	173	3512
Adsorbed gas, poisonous, n.o.s. (Inhalation hazard zone C)	173	3512
Adsorbed gas, poisonous, n.o.s. (Inhalation hazard zone D)	173	3512
Adsorbed gas, poisonous, oxidizing, corrosive, n.o.s.	173	3518
Adsorbed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation hazard zone A)	173	3518
Adsorbed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation hazard zone B)	173	3518
Adsorbed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation hazard zone C)	173	3518
Adsorbed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation hazard zone D)	173	3518
Adsorbed gas, poisonous, oxidizing, n.o.s.	173	3515
Adsorbed gas, poisonous, oxidizing, n.o.s. (Inhalation hazard zone A)	173	3515
Adsorbed gas, poisonous, oxidizing, n.o.s. (Inhalation hazard zone B)	173	3515
Adsorbed gas, poisonous, oxidizing, n.o.s. (Inhalation hazard zone C)	173	3515
Adsorbed gas, poisonous, oxidizing, n.o.s. (Inhalation hazard zone D)	173	3515
Adsorbed gas, toxic, corrosive, n.o.s.	173	3516
Adsorbed gas, toxic, corrosive, n.o.s. (Inhalation hazard zone A)	173	3516
Adsorbed gas, toxic, corrosive, n.o.s. (Inhalation hazard zone B)	173	3516
Adsorbed gas, toxic, corrosive, n.o.s. (Inhalation hazard zone C)	173	3516
Adsorbed gas, toxic, corrosive, n.o.s. (Inhalation hazard zone D)	173	3516
Adsorbed gas, toxic, flammable, corrosive, n.o.s.	173	3517
Adsorbed gas, toxic, flammable, corrosive, n.o.s. (Inhalation hazard zone A)	173	3517
Adsorbed gas, toxic, flammable, corrosive, n.o.s. (Inhalation hazard zone B)	173	3517
Adsorbed gas, toxic, flammable, corrosive, n.o.s. (Inhalation hazard zone C)	173	3517
Adsorbed gas, toxic, flammable, corrosive, n.o.s. (Inhalation hazard zone D)	173	3517

Name of Material	Guide No.	ID No.
Adsorbed gas, toxic, flammable, n.o.s.	173	3514
Adsorbed gas, toxic, flammable, n.o.s. (Inhalation hazard zone A)	173	3514
Adsorbed gas, toxic, flammable, n.o.s. (Inhalation hazard zone B)	173	3514
Adsorbed gas, toxic, flammable, n.o.s. (Inhalation hazard zone C)	173	3514
Adsorbed gas, toxic, flammable, n.o.s. (Inhalation hazard zone D)	173	3514
Adsorbed gas, toxic, n.o.s.	173	3512
Adsorbed gas, toxic, n.o.s. (Inhalation hazard zone A)	173	3512
Adsorbed gas, toxic, n.o.s. (Inhalation hazard zone B)	173	3512
Adsorbed gas, toxic, n.o.s. (Inhalation hazard zone C)	173	3512
Adsorbed gas, toxic, n.o.s. (Inhalation hazard zone D)	173	3512
Adsorbed gas, toxic, oxidizing, corrosive, n.o.s.	173	3518
Adsorbed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation hazard zone A)	173	3518
Adsorbed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation hazard zone B)	173	3518
Adsorbed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation hazard zone C)	173	3518
Adsorbed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation hazard zone D)	173	3518
Adsorbed gas, toxic, oxidizing, n.o.s.	173	3515
Adsorbed gas, toxic, oxidizing, n.o.s. (Inhalation hazard zone A)	173	3515
Adsorbed gas, toxic, oxidizing, n.o.s. (Inhalation hazard zone B)	173	3515
Adsorbed gas, toxic, oxidizing, n.o.s. (Inhalation hazard zone C)	173	3515
Adsorbed gas, toxic, oxidizing, n.o.s. (Inhalation hazard zone D)	173	3515
Aerosols	126	1950
Air, compressed	122	1002
Air, refrigerated liquid (cryogenic liquid)	122	1003
Air bag inflators	171	3268
Air bag modules	171	3268
Aircraft hydraulic power unit fuel tank	131	3165
Alcoholates solution, n.o.s., in alcohol	132	3274
Alcoholic beverages	127	3065
Alcohols, flammable, poisonous, n.o.s.	131	1986
Alcohols, flammable, toxic, n.o.s.	131	1986
Alcohols, n.o.s.	127	1987
Aldehydes, flammable, poisonous, n.o.s.	131P	1988
Aldehydes, flammable, toxic, n.o.s.	131P	1988
Aldehydes, n.o.s.	129P	1989
Aldol	153	2839
Alkali metal alcoholates, self-heating, corrosive, n.o.s.	136	3206
Alkali metal alloy, liquid, n.o.s.	138	1421
Alkali metal amalgam, liquid	138	1389
Alkali metal amalgam, solid	138	3401
Alkali metal amides	139	1390

Name of Material	Guide No.	ID No.
Alkali metal dispersion	**138**	1391
Alkali metal dispersion, flammable	**138**	3482
Alkaline earth metal alcoholates, n.o.s.	**135**	3205
Alkaline earth metal alloy, n.o.s.	**138**	1393
Alkaline earth metal amalgam, liquid	**138**	1392
Alkaline earth metal amalgam, solid	**138**	3402
Alkaline earth metal dispersion	**138**	1391
Alkaline earth metal dispersion, flammable	**138**	3482
Alkaloids, liquid, n.o.s. (poisonous)	**151**	3140
Alkaloids, solid, n.o.s. (poisonous)	**151**	1544
Alkaloid salts, liquid, n.o.s. (poisonous)	**151**	3140
Alkaloid salts, solid, n.o.s. (poisonous)	**151**	1544
Alkylphenols, liquid, n.o.s. (including C2-C12 homologues)	**153**	3145
Alkylphenols, solid, n.o.s. (including C2-C12 homologues)	**153**	2430
Alkyl sulfonic acids, liquid, with more than 5% free Sulfuric acid	**153**	2584
Alkyl sulfonic acids, liquid, with not more than 5% free Sulfuric acid	**153**	2586
Alkyl sulfonic acids, solid, with more than 5% free Sulfuric acid	**153**	2583
Alkyl sulfonic acids, solid, with not more than 5% free Sulfuric acid	**153**	2585
Alkylsulfuric acids	**156**	2571
Alkyl sulphonic acids, liquid, with more than 5% free Sulphuric acid	**153**	2584
Alkyl sulphonic acids, liquid, with not more than 5% free Sulphuric acid	**153**	2586
Alkyl sulphonic acids, solid, with more than 5% free Sulphuric acid	**153**	2583
Alkyl sulphonic acids, solid, with not more than 5% free Sulphuric acid	**153**	2585
Alkylsulphuric acids	**156**	2571
Allyl acetate	**131**	2333
Allyl alcohol	**131**	1098
Allylamine	**131**	2334
Allyl bromide	**131P**	1099
Allyl chloride	**131P**	1100
Allyl chlorocarbonate	**155**	1722
Allyl chloroformate	**155**	1722
Allyl ethyl ether	**131**	2335
Allyl formate	**131**	2336
Allyl glycidyl ether	**129**	2219
Allyl iodide	**132**	1723
Allyl isothiocyanate, stabilized	**155**	1545
Allyltrichlorosilane, stabilized	**155**	1724
alpha-Methylbenzyl alcohol, liquid	**153**	2937
alpha-Methylbenzyl alcohol, solid	**153**	3438
alpha-Methylvaleraldehyde	**130**	2367
alpha-Naphthylamine	**153**	2077
alpha-Pinene	**128**	2368
Aluminum, molten	**169**	9260
Aluminum alkyl hydrides	**138**	3076
Aluminum alkyls	**135**	3051

Name of Material	Guide No.	ID No.
Aluminum borohydride	135	2870
Aluminum borohydride in devices	135	2870
Aluminum bromide, anhydrous	137	1725
Aluminum bromide, solution	154	2580
Aluminum carbide	138	1394
Aluminum chloride, anhydrous	137	1726
Aluminum chloride, solution	154	2581
Aluminum dross	138	3170
Aluminum ferrosilicon powder	139	1395
Aluminum hydride	138	2463
Aluminum nitrate	140	1438
Aluminum phosphide	139	1397
Aluminum phosphide pesticide	157	3048
Aluminum powder, coated	170	1309
Aluminum powder, pyrophoric	135	1383
Aluminum powder, uncoated	138	1396
Aluminum remelting by-products	138	3170
Aluminum resinate	133	2715
Aluminum silicon powder, uncoated	138	1398
Aluminum smelting by-products	138	3170
Amines, flammable, corrosive, n.o.s.	132	2733
Amines, liquid, corrosive, flammable, n.o.s.	132	2734
Amines, liquid, corrosive, n.o.s.	153	2735
Amines, solid, corrosive, n.o.s.	154	3259
2-Amino-4-chlorophenol	151	2673
2-Amino-5-diethylaminopentane	153	2946
2-Amino-4,6-dinitrophenol, wetted with not less than 20% water	113	3317
2-(2-Aminoethoxy)ethanol	154	3055
N-Aminoethylpiperazine	153	2815
Aminophenols	152	2512
Aminopyridines	153	2671
Ammonia, anhydrous	125	1005
Ammonia, solution, with more than 10% but not more than 35% Ammonia	154	2672
Ammonia, solution, with more than 35% but not more than 50% Ammonia	125	2073
Ammonia solution, with more than 50% Ammonia	125	3318
Ammonium arsenate	151	1546
Ammonium bifluoride, solid	154	1727
Ammonium bifluoride, solution	154	2817
Ammonium dichromate	141	1439
Ammonium dinitro-o-cresolate, solid	141	1843
Ammonium dinitro-o-cresolate, solution	141	3424
Ammonium fluoride	154	2505
Ammonium fluorosilicate	151	2854
Ammonium hydrogendifluoride, solid	154	1727
Ammonium hydrogendifluoride, solution	154	2817
Ammonium hydrogen sulfate	154	2506
Ammonium hydrogen sulphate	154	2506
Ammonium hydroxide	154	2672
Ammonium hydroxide, with more than 10% but not more than 35% Ammonia	154	2672
Ammonium metavanadate	154	2859
Ammonium nitrate, liquid (hot concentrated solution)	140	2426

Name of Material	Guide No.	ID No.
Ammonium nitrate, with not more than 0.2% combustible substances	**140**	1942
Ammonium nitrate based fertilizer	**140**	2067
Ammonium nitrate based fertilizer	**140**	2071
Ammonium nitrate emulsion	**140**	3375
Ammonium nitrate-fuel oil mixtures	**112**	——
Ammonium nitrate gel	**140**	3375
Ammonium nitrate suspension	**140**	3375
Ammonium perchlorate	**143**	1442
Ammonium persulfate	**140**	1444
Ammonium persulphate	**140**	1444
Ammonium picrate, wetted with not less than 10% water	**113**	1310
Ammonium polysulfide, solution	**154**	2818
Ammonium polysulphide, solution	**154**	2818
Ammonium polyvanadate	**151**	2861
Ammonium silicofluoride	**151**	2854
Ammonium sulfide, solution	**132**	2683
Ammonium sulphide, solution	**132**	2683
Ammunition, poisonous, non-explosive	**151**	2016
Ammunition, tear-producing, non-explosive	**159**	2017
Ammunition, toxic, non-explosive	**151**	2016
Amyl acetates	**129**	1104
Amyl acid phosphate	**153**	2819
Amylamine	**132**	1106
Amyl butyrates	**130**	2620
Amyl chloride	**129**	1107
n-Amylene	**128**	1108
Amyl formates	**129**	1109
Amyl mercaptan	**130**	1111
n-Amyl methyl ketone	**127**	1110
Amyl nitrate	**128**	1112
Amyl nitrite	**129**	1113
Amyltrichlorosilane	**155**	1728
Anhydrous ammonia	**125**	1005
Aniline	**153**	1547
Aniline hydrochloride	**153**	1548
Anisidines	**153**	2431
Anisole	**128**	2222
Anisoyl chloride	**156**	1729
Antimony compound, inorganic, liquid, n.o.s.	**157**	3141
Antimony compound, inorganic, solid, n.o.s.	**157**	1549
Antimony lactate	**151**	1550
Antimony pentachloride, liquid	**157**	1730
Antimony pentachloride, solution	**157**	1731
Antimony pentafluoride	**157**	1732
Antimony potassium tartrate	**151**	1551
Antimony powder	**170**	2871
Antimony trichloride	**157**	1733
Antimony trichloride, liquid	**157**	1733
Antimony trichloride, solid	**157**	1733
Aqua regia	**157**	1798
Argon	**120**	1006
Argon, compressed	**120**	1006
Argon, refrigerated liquid (cryogenic liquid)	**120**	1951
Arsenic	**152**	1558

Name of Material	Guide No.	ID No.
Arsenic acid, liquid	154	1553
Arsenic acid, solid	154	1554
Arsenical dust	152	1562
Arsenical pesticide, liquid, flammable, poisonous	131	2760
Arsenical pesticide, liquid, flammable, toxic	131	2760
Arsenical pesticide, liquid, poisonous	151	2994
Arsenical pesticide, liquid, poisonous, flammable	131	2993
Arsenical pesticide, liquid, toxic	151	2994
Arsenical pesticide, liquid, toxic, flammable	131	2993
Arsenical pesticide, solid, poisonous	151	2759
Arsenical pesticide, solid, toxic	151	2759
Arsenic bromide	151	1555
Arsenic chloride	157	1560
Arsenic compound, liquid, n.o.s.	152	1556
Arsenic compound, solid, n.o.s.	152	1557
Arsenic pentoxide	151	1559
Arsenic trichloride	157	1560
Arsenic trioxide	151	1561
Arsine	119	2188
Arsine, adsorbed	173	3522
Articles containing a substance liable to spontaneous combustion, n.o.s.	135	3542
Articles containing a substance which emits flammable gas in contact with water, n.o.s.	138	3543
Articles containing corrosive substance, n.o.s.	154	3547
Articles containing flammable gas, n.o.s.	115	3537
Articles containing flammable liquid, n.o.s.	127	3540
Articles containing flammable solid, n.o.s.	133	3541
Articles containing miscellaneous dangerous goods, n.o.s.	171	3548
Articles containing non-flammable, non-toxic gas, n.o.s.	120	3538
Articles containing oxidizing substance, n.o.s.	140	3544
Articles containing organic peroxide, n.o.s.	145	3545
Articles containing Polychlorinated biphenyls (PCB)	171	2315
Articles containing toxic gas, n.o.s.	123	3539
Articles containing toxic substance, n.o.s.	151	3546
Articles, pressurized, hydraulic (containing non-flammable gas)	126	3164
Articles, pressurized, pneumatic (containing non-flammable gas)	126	3164
Aryl sulfonic acids, liquid, with more than 5% free Sulfuric acid	153	2584
Aryl sulfonic acids, liquid, with not more than 5% free Sulfuric acid	153	2586
Aryl sulfonic acids, solid, with more than 5% free Sulfuric acid	153	2583
Aryl sulfonic acids, solid, with not more than 5% free Sulfuric acid	153	2585

Name of Material	Guide No.	ID No.
Aryl sulphonic acids, liquid, with more than 5% free Sulphuric acid	**153**	2584
Aryl sulphonic acids, liquid, with not more than 5% free Sulphuric acid	**153**	2586
Aryl sulphonic acids, solid, with more than 5% free Sulphuric acid	**153**	2583
Aryl sulphonic acids, solid, with not more than 5% free Sulphuric acid	**153**	2585
Asbestos	**171**	2212
Asbestos, amphibole	**171**	2212
Asbestos, blue	**171**	2212
Asbestos, brown	**171**	2212
Asbestos, chrysotile	**171**	2590
Asbestos, white	**171**	2590
Asphalt	**130**	1999
Asphalt, cut back	**130**	1999
Aviation regulated liquid, n.o.s.	**171**	3334
Aviation regulated solid, n.o.s.	**171**	3335
Azodicarbonamide	**149**	3242
Barium	**138**	1400
Barium alloys, pyrophoric	**135**	1854
Barium azide, wetted with not less than 50% water	**113**	1571
Barium bromate	**141**	2719
Barium chlorate, solid	**141**	1445
Barium chlorate, solution	**141**	3405
Barium compound, n.o.s.	**154**	1564
Barium cyanide	**157**	1565
Barium hypochlorite, with more than 22% available Chlorine	**141**	2741
Barium nitrate	**141**	1446
Barium oxide	**157**	1884
Barium perchlorate, solid	**141**	1447
Barium perchlorate, solution	**141**	3406
Barium permanganate	**141**	1448
Barium peroxide	**141**	1449
Batteries, containing Sodium	**138**	3292
Batteries, dry, containing Potassium hydroxide solid	**154**	3028
Batteries, nickel-metal hydride	**171**	3496
Batteries, wet, filled with acid	**154**	2794
Batteries, wet, filled with alkali	**154**	2795
Batteries, wet, non-spillable	**154**	2800
Battery fluid, acid	**157**	2796
Battery fluid, alkali	**154**	2797
Battery-powered equipment (wet battery)	**154**	3171
Battery-powered equipment (with lithium ion batteries)	**147**	3171
Battery-powered equipment (with lithium metal batteries)	**138**	3171
Battery-powered equipment (with sodium batteries)	**138**	3171
Battery-powered vehicle (wet battery)	**154**	3171
Battery-powered vehicle (with lithium ion batteries)	**147**	3171
Battery-powered vehicle (with sodium batteries)	**138**	3171
Benzaldehyde	**171**	1990
Benzene	**130**	1114
Benzene phosphorus dichloride	**137**	2798
Benzene phosphorus thiodichloride	**137**	2799
Benzenesulfonyl chloride	**156**	2225
Benzenesulphonyl chloride	**156**	2225
Benzidine	**153**	1885
Benzonitrile	**152**	2224

Name of Material	Guide No.	ID No.
Benzoquinone	153	2587
Benzotrichloride	156	2226
Benzotrifluoride	127	2338
Benzoyl chloride	137	1736
Benzyl bromide	156	1737
Benzyl chloride	156	1738
Benzyl chloroformate	137	1739
Benzyldimethylamine	132	2619
Benzylidene chloride	156	1886
Benzyl iodide	156	2653
Beryllium compound, n.o.s.	154	1566
Beryllium nitrate	141	2464
Beryllium powder	134	1567
beta-Naphthylamine, solid	153	1650
beta-Naphthylamine, solution	153	3411
Bhusa, wet, damp or contaminated with oil	133	1327
Bicyclo[2.2.1]hepta-2,5-diene, stabilized	128P	2251
Biological agents	158	——
Biological substance, category B	158	3373
(Bio)Medical waste, n.o.s.	158	3291
Bipyridilium pesticide, liquid, flammable, poisonous	131	2782
Bipyridilium pesticide, liquid, flammable, toxic	131	2782
Bipyridilium pesticide, liquid, poisonous	151	3016
Bipyridilium pesticide, liquid, poisonous, flammable	131	3015
Bipyridilium pesticide, liquid, toxic	151	3016
Bipyridilium pesticide, liquid, toxic, flammable	131	3015
Bipyridilium pesticide, solid, poisonous	151	2781
Bipyridilium pesticide, solid, toxic	151	2781
Bisulfates, aqueous solution	154	2837
Bisulfites, aqueous solution, n.o.s.	154	2693
Bisulphates, aqueous solution	154	2837
Bisulphites, aqueous solution, n.o.s.	154	2693
Blasting agent, n.o.s.	112	——
Bleaching powder	140	2208
Blue asbestos	171	2212
Bombs, smoke, non-explosive, with corrosive liquid, without initiating device	153	2028
Borate and Chlorate mixture	140	1458
Borneol	133	1312
Boron tribromide	157	2692
Boron trichloride	125	1741
Boron trifluoride	125	1008
Boron trifluoride, adsorbed	173	3519
Boron trifluoride, compressed	125	1008
Boron trifluoride, dihydrate	157	2851
Boron trifluoride acetic acid complex, liquid	157	1742
Boron trifluoride acetic acid complex, solid	157	3419
Boron trifluoride diethyl etherate	132	2604
Boron trifluoride dimethyl etherate	139	2965
Boron trifluoride propionic acid complex, liquid	157	1743
Boron trifluoride propionic acid complex, solid	157	3420

Name of Material	Guide No.	ID No.
Bromates, inorganic, aqueous solution, n.o.s.	140	3213
Bromates, inorganic, n.o.s.	140	1450
Bromine	154	1744
Bromine, solution	154	1744
Bromine, solution (Inhalation Hazard Zone A)	154	1744
Bromine, solution (Inhalation Hazard Zone B)	154	1744
Bromine chloride	124	2901
Bromine pentafluoride	144	1745
Bromine trifluoride	144	1746
Bromoacetic acid, solid	156	3425
Bromoacetic acid, solution	156	1938
Bromoacetone	131	1569
Bromoacetyl bromide	156	2513
Bromobenzene	130	2514
Bromobenzyl cyanides, liquid	159	1694
Bromobenzyl cyanides, solid	159	3449
1-Bromobutane	130	1126
2-Bromobutane	130	2339
Bromochloromethane	160	1887
1-Bromo-3-chloropropane	159	2688
2-Bromoethyl ethyl ether	130	2340
Bromoform	159	2515
1-Bromo-3-methylbutane	130	2341
Bromomethylpropanes	130	2342
2-Bromo-2-nitropropane-1,3-diol	133	3241
2-Bromopentane	130	2343
Bromopropanes	129	2344
3-Bromopropyne	130	2345
Bromotrifluoroethylene	116	2419
Bromotrifluoromethane	126	1009
Brown asbestos	171	2212
Brucine	152	1570
Butadienes, stabilized	116P	1010
Butadienes and hydrocarbon mixture, stabilized	116P	1010
Butane	115	1011
Butane	115	1075
Butanedione	127	2346
Butanols	129	1120
Butyl acetates	129	1123
Butyl acid phosphate	153	1718
Butyl acrylates, stabilized	129P	2348
n-Butylamine	132	1125
N-Butylaniline	153	2738
Butylbenzenes	128	2709
n-Butyl bromide	130	1126
n-Butyl chloride	130	1127
n-Butyl chloroformate	155	2743
sec-Butyl chloroformate	155	2742
tert-Butylcyclohexyl chloroformate	156	2747
Butylene	115	1012
Butylene	115	1075
1,2-Butylene oxide, stabilized	127P	3022
Butyl ethers	128	1149
n-Butyl formate	129	1128
tert-Butyl hypochlorite	135	3255
N,n-Butylimidazole	152	2690
n-Butyl isocyanate	155P	2485
tert-Butyl isocyanate	155	2484
Butyl mercaptan	130	2347

Name of Material	Guide No.	ID No.
n-Butyl methacrylate, stabilized	130P	2227
Butyl methyl ether	127	2350
Butyl nitrites	129	2351
Butyl propionates	130	1914
Butyltoluenes	152	2667
Butyltrichlorosilane	155	1747
5-tert-Butyl-2,4,6-trinitro-m-xylene	149	2956
Butyl vinyl ether, stabilized	127P	2352
1,4-Butynediol	153	2716
Butyraldehyde	129P	1129
Butyraldoxime	129	2840
Butyric acid	153	2820
Butyric anhydride	156	2739
Butyronitrile	131	2411
Butyryl chloride	132	2353
Buzz	153	——
BZ	153	——
CA	159	——
Cacodylic acid	151	1572
Cadmium compound	154	2570
Caesium	138	1407
Caesium hydroxide	157	2682
Caesium hydroxide, solution	154	2681
Caesium nitrate	140	1451
Calcium	138	1401
Calcium, pyrophoric	135	1855
Calcium alloys, pyrophoric	135	1855
Calcium arsenate	151	1573
Calcium arsenate and Calcium arsenite mixture, solid	151	1574
Calcium arsenite and Calcium arsenate mixture, solid	151	1574
Calcium carbide	138	1402
Calcium chlorate	140	1452
Calcium chlorate, aqueous solution	140	2429
Calcium chlorite	140	1453
Calcium cyanamide, with more than 0.1% Calcium carbide	138	1403
Calcium cyanide	157	1575
Calcium dithionite	135	1923
Calcium hydride	138	1404
Calcium hydrosulfite	135	1923
Calcium hydrosulphite	135	1923
Calcium hypochlorite, dry	140	1748
Calcium hypochlorite, dry, corrosive, with more than 39% available chlorine (8.8% available oxygen)	140	3485
Calcium hypochlorite, hydrated, corrosive, with not less than 5.5% but not more than 16% water	140	3487
Calcium hypochlorite, hydrated, with not less than 5.5% but not more than 16% water	140	2880
Calcium hypochlorite, hydrated mixture, corrosive, with not less than 5.5% but not more than 16% water	140	3487
Calcium hypochlorite, hydrated mixture, with not less than 5.5% but not more than 16% water	140	2880
Calcium hypochlorite mixture, dry, corrosive, with more than 10% but not more than 39% available chlorine	140	3486

Name of Material	Guide No.	ID No.
Calcium hypochlorite mixture, dry, corrosive, with more than 39% available chlorine (8.8% available oxygen)	140	3485
Calcium hypochlorite mixture, dry, with more than 10% but not more than 39% available Chlorine	140	2208
Calcium hypochlorite mixture, dry, with more than 39% available Chlorine (8.8% available Oxygen)	140	1748
Calcium manganese silicon	138	2844
Calcium nitrate	140	1454
Calcium oxide	157	1910
Calcium perchlorate	140	1455
Calcium permanganate	140	1456
Calcium peroxide	140	1457
Calcium phosphide	139	1360
Calcium resinate	133	1313
Calcium resinate, fused	133	1314
Calcium silicide	138	1405
Camphor, synthetic	133	2717
Camphor oil	128	1130
Capacitor, asymmetric	171	3508
Capacitor, electric double layer	171	3499
Caproic acid	153	2829
Carbamate pesticide, liquid, flammable, poisonous	131	2758
Carbamate pesticide, liquid, flammable, toxic	131	2758
Carbamate pesticide, liquid, poisonous	151	2992
Carbamate pesticide, liquid, poisonous, flammable	131	2991
Carbamate pesticide, liquid, toxic	151	2992
Carbamate pesticide, liquid, toxic, flammable	131	2991
Carbamate pesticide, solid, poisonous	151	2757
Carbamate pesticide, solid, toxic	151	2757
Carbon, activated	133	1362
Carbon, animal or vegetable origin	133	1361
Carbon bisulfide	131	1131
Carbon bisulphide	131	1131
Carbon dioxide	120	1013
Carbon dioxide, compressed	120	1013
Carbon dioxide, refrigerated liquid	120	2187
Carbon dioxide, solid	120	1845
Carbon dioxide and Ethylene oxide mixture, with more than 9% but not more than 87% Ethylene oxide	115	1041
Carbon dioxide and Ethylene oxide mixture, with more than 87% Ethylene oxide	119P	3300
Carbon dioxide and Ethylene oxide mixtures, with not more than 9% Ethylene oxide	126	1952
Carbon dioxide and Nitrous oxide mixture	126	1015
Carbon dioxide and Oxygen mixture, compressed	122	1014
Carbon disulfide	131	1131
Carbon disulphide	131	1131
Carbon monoxide	119	1016
Carbon monoxide, compressed	119	1016
Carbon monoxide, refrigerated liquid (cryogenic liquid)	168	9202
Carbon tetrabromide	151	2516
Carbon tetrachloride	151	1846

Name of Material	Guide No.	ID No.
Carbonyl fluoride	125	2417
Carbonyl fluoride, compressed	125	2417
Carbonyl sulfide	119	2204
Carbonyl sulphide	119	2204
Castor beans, meal, pomace or flake	171	2969
Caustic alkali liquid, n.o.s.	154	1719
Caustic potash, solid	154	1813
Caustic potash, solution	154	1814
Caustic soda, solid	154	1823
Caustic soda, solution	154	1824
Cells, containing Sodium	138	3292
Celluloid, in blocks, rods, rolls, sheets, tubes, etc., except scrap	133	2000
Celluloid, scrap	135	2002
Cerium, slabs, ingots or rods	170	1333
Cerium, turnings or gritty powder	138	3078
Cesium	138	1407
Cesium hydroxide	157	2682
Cesium hydroxide, solution	154	2681
Cesium nitrate	140	1451
CG	125	——
Charcoal	133	1361
Chemical kit	154	1760
Chemical kit	171	3316
Chemical sample, poisonous	151	3315
Chemical sample, toxic	151	3315
Chemical under pressure, corrosive, n.o.s.	125	3503
Chemical under pressure, flammable, corrosive, n.o.s.	118	3505
Chemical under pressure, flammable, n.o.s.	115	3501
Chemical under pressure, flammable, poisonous, n.o.s.	119	3504
Chemical under pressure, flammable, toxic, n.o.s.	119	3504
Chemical under pressure, n.o.s.	126	3500
Chemical under pressure, poisonous, n.o.s.	123	3502
Chemical under pressure, toxic, n.o.s.	123	3502
Chloral, anhydrous, stabilized	153	2075
Chlorate and Borate mixture	140	1458
Chlorate and Magnesium chloride mixture, solid	140	1459
Chlorate and Magnesium chloride mixture, solution	140	3407
Chlorates, inorganic, aqueous solution, n.o.s.	140	3210
Chlorates, inorganic, n.o.s.	140	1461
Chloric acid, aqueous solution, with not more than 10% Chloric acid	140	2626
Chlorine	124	1017
Chlorine, adsorbed	173	3520
Chlorine dioxide, hydrate, frozen	143	9191
Chlorine pentafluoride	124	2548
Chlorine trifluoride	124	1749
Chlorite solution	154	1908
Chlorites, inorganic, n.o.s.	143	1462
Chloroacetaldehyde	153	2232
Chloroacetic acid, molten	153	3250
Chloroacetic acid, solid	153	1751
Chloroacetic acid, solution	153	1750
Chloroacetone, stabilized	131	1695
Chloroacetonitrile	131	2668

Name of Material	Guide No.	ID No.
Chloroacetophenone, liquid	153	3416
Chloroacetophenone, solid	153	1697
Chloroacetyl chloride	156	1752
Chloroanilines, liquid	152	2019
Chloroanilines, solid	152	2018
Chloroanisidines	152	2233
Chlorobenzene	130	1134
Chlorobenzotrifluorides	130	2234
Chlorobenzyl chlorides, liquid	153	2235
Chlorobenzyl chlorides, solid	153	3427
Chlorobutanes	130	1127
Chlorocresols, solid	152	3437
Chlorocresols, solution	152	2669
Chlorodifluorobromomethane	126	1974
1-Chloro-1,1-difluoroethane	115	2517
Chlorodifluoromethane	126	1018
Chlorodifluoromethane and Chloropentafluoroethane mixture	126	1973
Chlorodinitrobenzenes, liquid	153	1577
Chlorodinitrobenzenes, solid	153	3441
2-Chloroethanal	153	2232
Chloroform	151	1888
Chloroformates, poisonous, corrosive, flammable, n.o.s.	155	2742
Chloroformates, poisonous, corrosive, n.o.s.	154	3277
Chloroformates, toxic, corrosive, flammable, n.o.s.	155	2742
Chloroformates, toxic, corrosive, n.o.s.	154	3277
Chloromethyl chloroformate	157	2745
Chloromethyl ethyl ether	131	2354
3-Chloro-4-methylphenyl isocyanate, liquid	156	2236
3-Chloro-4-methylphenyl isocyanate, solid	156	3428
Chloronitroanilines	153	2237
Chloronitrobenzenes, liquid	152	3409
Chloronitrobenzenes, solid	152	1578
Chloronitrotoluenes, liquid	152	2433
Chloronitrotoluenes, solid	152	3457
Chloropentafluoroethane	126	1020
Chloropentafluoroethane and Chlorodifluoromethane mixture	126	1973
Chlorophenolates, liquid	154	2904
Chlorophenolates, solid	154	2905
Chlorophenols, liquid	153	2021
Chlorophenols, solid	153	2020
Chlorophenyltrichlorosilane	156	1753
Chloropicrin	154	1580
Chloropicrin and Methyl bromide mixture	123	1581
Chloropicrin and Methyl chloride mixture	119	1582
Chloropicrin mixture, n.o.s.	154	1583
Chloropivaloyl chloride	156	9263
Chloroplatinic acid, solid	154	2507
Chloroprene, stabilized	131P	1991
1-Chloropropane	129	1278
2-Chloropropane	129	2356
3-Chloropropanol-1	153	2849
2-Chloropropene	130P	2456
2-Chloropropionic acid	153	2511
2-Chloropyridine	153	2822
Chlorosilanes, corrosive, flammable, n.o.s.	155	2986
Chlorosilanes, corrosive, n.o.s.	156	2987

Name of Material	Guide No.	ID No.
Chlorosilanes, flammable, corrosive, n.o.s.	155	2985
Chlorosilanes, poisonous, corrosive, flammable, n.o.s.	155	3362
Chlorosilanes, poisonous, corrosive, n.o.s.	156	3361
Chlorosilanes, toxic, corrosive, flammable, n.o.s.	155	3362
Chlorosilanes, toxic, corrosive, n.o.s.	156	3361
Chlorosilanes, water-reactive, flammable, corrosive, n.o.s.	139	2988
Chlorosulfonic acid (with or without sulfur trioxide)	137	1754
Chlorosulphonic acid (with or without sulphur trioxide)	137	1754
1-Chloro-1,2,2,2-tetrafluoroethane	126	1021
Chlorotetrafluoroethane and Ethylene oxide mixture, with not more than 8.8% Ethylene oxide	126	3297
Chlorotoluenes	129	2238
4-Chloro-o-toluidine hydrochloride, solid	153	1579
4-Chloro-o-toluidine hydrochloride, solution	153	3410
Chlorotoluidines, liquid	153	3429
Chlorotoluidines, solid	153	2239
1-Chloro-2,2,2-trifluoroethane	126	1983
Chlorotrifluoromethane	126	1022
Chlorotrifluoromethane and Trifluoromethane azeotropic mixture with approximately 60% Chlorotrifluoromethane	126	2599
Chromic acid, solution	154	1755
Chromic fluoride, solid	154	1756
Chromic fluoride, solution	154	1757
Chromium nitrate	141	2720
Chromium oxychloride	137	1758
Chromium trioxide, anhydrous	141	1463
Chromosulfuric acid	154	2240
Chromosulphuric acid	154	2240
CK	125	——
Clinical waste, unspecified, n.o.s.	158	3291
CN	153	——
Coal gas	119	1023
Coal gas, compressed	119	1023
Coal tar distillates, flammable	128	1136
Coating solution	127	1139
Cobalt naphthenates, powder	133	2001
Cobalt resinate, precipitated	133	1318
Combustible liquid, n.o.s.	128	1993
Compounds, cleaning liquid (corrosive)	154	1760
Compounds, cleaning liquid (flammable)	128	1993
Compounds, tree or weed killing, liquid (corrosive)	154	1760
Compounds, tree or weed killing, liquid (flammable)	128	1993
Compounds, tree or weed killing, liquid (toxic)	153	2810
Compressed gas, flammable, n.o.s.	115	1954
Compressed gas, n.o.s.	126	1956
Compressed gas, oxidizing, n.o.s.	122	3156
Compressed gas, poisonous, corrosive, n.o.s.	125	3304
Compressed gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone A)	125	3304

Name of Material	Guide No.	ID No.
Compressed gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone B)	125	3304
Compressed gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone C)	125	3304
Compressed gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone D)	125	3304
Compressed gas, poisonous, flammable, corrosive, n.o.s.	119	3305
Compressed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)	119	3305
Compressed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)	119	3305
Compressed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone C)	119	3305
Compressed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone D)	119	3305
Compressed gas, poisonous, flammable, n.o.s.	119	1953
Compressed gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone A)	119	1953
Compressed gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone B)	119	1953
Compressed gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone C)	119	1953
Compressed gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone D)	119	1953
Compressed gas, poisonous, n.o.s.	123	1955
Compressed gas, poisonous, n.o.s. (Inhalation Hazard Zone A)	123	1955
Compressed gas, poisonous, n.o.s. (Inhalation Hazard Zone B)	123	1955
Compressed gas, poisonous, n.o.s. (Inhalation Hazard Zone C)	123	1955
Compressed gas, poisonous, n.o.s. (Inhalation Hazard Zone D)	123	1955
Compressed gas, poisonous, oxidizing, corrosive, n.o.s.	124	3306
Compressed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone A)	124	3306
Compressed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone B)	124	3306
Compressed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone C)	124	3306
Compressed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone D)	124	3306
Compressed gas, poisonous, oxidizing, n.o.s.	124	3303
Compressed gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone A)	124	3303
Compressed gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone B)	124	3303
Compressed gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone C)	124	3303
Compressed gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone D)	124	3303
Compressed gas, toxic, corrosive, n.o.s.	125	3304
Compressed gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone A)	125	3304

Name of Material	Guide No.	ID No.
Compressed gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone B)	125	3304
Compressed gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone C)	125	3304
Compressed gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone D)	125	3304
Compressed gas, toxic, flammable, corrosive, n.o.s.	119	3305
Compressed gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)	119	3305
Compressed gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)	119	3305
Compressed gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone C)	119	3305
Compressed gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone D)	119	3305
Compressed gas, toxic, flammable, n.o.s.	119	1953
Compressed gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone A)	119	1953
Compressed gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone B)	119	1953
Compressed gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone C)	119	1953
Compressed gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone D)	119	1953
Compressed gas, toxic, n.o.s.	123	1955
Compressed gas, toxic, n.o.s. (Inhalation Hazard Zone A)	123	1955
Compressed gas, toxic, n.o.s. (Inhalation Hazard Zone B)	123	1955
Compressed gas, toxic, n.o.s. (Inhalation Hazard Zone C)	123	1955
Compressed gas, toxic, n.o.s. (Inhalation Hazard Zone D)	123	1955
Compressed gas, toxic, oxidizing, corrosive, n.o.s.	124	3306
Compressed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone A)	124	3306
Compressed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone B)	124	3306
Compressed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone C)	124	3306
Compressed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone D)	124	3306
Compressed gas, toxic, oxidizing, n.o.s.	124	3303
Compressed gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone A)	124	3303
Compressed gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone B)	124	3303
Compressed gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone C)	124	3303
Compressed gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone D)	124	3303
Compressed gas and hexaethyl tetraphosphate mixture	123	1612
Consumer commodity	171	8000
Copper acetoarsenite	151	1585
Copper arsenite	151	1586
Copper based pesticide, liquid, flammable, poisonous	131	2776
Copper based pesticide, liquid, flammable, toxic	131	2776

Name of Material	Guide No.	ID No.
Copper based pesticide, liquid, poisonous	**151**	3010
Copper based pesticide, liquid, poisonous, flammable	**131**	3009
Copper based pesticide, liquid, toxic	**151**	3010
Copper based pesticide, liquid, toxic, flammable	**131**	3009
Copper based pesticide, solid, poisonous	**151**	2775
Copper based pesticide, solid, toxic	**151**	2775
Copper chlorate	**140**	2721
Copper chloride	**154**	2802
Copper cyanide	**151**	1587
Copra	**135**	1363
Corrosive liquid, acidic, inorganic, n.o.s.	**154**	3264
Corrosive liquid, acidic, organic, n.o.s.	**153**	3265
Corrosive liquid, basic, inorganic, n.o.s.	**154**	3266
Corrosive liquid, basic, organic, n.o.s.	**153**	3267
Corrosive liquid, flammable, n.o.s.	**132**	2920
Corrosive liquid, n.o.s.	**154**	1760
Corrosive liquid, oxidizing, n.o.s.	**157**	3093
Corrosive liquid, poisonous, n.o.s.	**154**	2922
Corrosive liquid, self-heating, n.o.s.	**136**	3301
Corrosive liquid, toxic, n.o.s.	**154**	2922
Corrosive liquid, water-reactive, n.o.s.	**138**	3094
Corrosive solid, acidic, inorganic, n.o.s.	**154**	3260
Corrosive solid, acidic, organic, n.o.s.	**154**	3261
Corrosive solid, basic, inorganic, n.o.s.	**154**	3262
Corrosive solid, basic, organic, n.o.s.	**154**	3263
Corrosive solid, flammable, n.o.s.	**134**	2921
Corrosive solid, n.o.s.	**154**	1759
Corrosive solid, oxidizing, n.o.s.	**157**	3084
Corrosive solid, poisonous, n.o.s.	**154**	2923
Corrosive solid, self-heating, n.o.s.	**136**	3095
Corrosive solid, toxic, n.o.s.	**154**	2923
Corrosive solid, water-reactive, n.o.s.	**138**	3096
Cotton	**133**	1365
Cotton, wet	**133**	1365
Cotton waste, oily	**133**	1364
Coumarin derivative pesticide, liquid, flammable, poisonous	**131**	3024
Coumarin derivative pesticide, liquid, flammable, toxic	**131**	3024
Coumarin derivative pesticide, liquid, poisonous	**151**	3026
Coumarin derivative pesticide, liquid, poisonous, flammable	**131**	3025
Coumarin derivative pesticide, liquid, toxic	**151**	3026
Coumarin derivative pesticide, liquid, toxic, flammable	**131**	3025
Coumarin derivative pesticide, solid, poisonous	**151**	3027
Coumarin derivative pesticide, solid, toxic	**151**	3027
Cresols, liquid	**153**	2076

Name of Material	Guide No.	ID No.
Cresols, solid	153	3455
Cresylic acid	153	2022
Crotonaldehyde	131P	1143
Crotonaldehyde, stabilized	131P	1143
Crotonic acid, liquid	153	3472
Crotonic acid, solid	153	2823
Crotonylene	128	1144
CS	153	——
Cumene	130	1918
Cupriethylenediamine, solution	154	1761
CX	154	——
Cyanide solution, n.o.s.	157	1935
Cyanides, inorganic, solid, n.o.s.	157	1588
Cyanogen	119	1026
Cyanogen bromide	157	1889
Cyanogen chloride, stabilized	125	1589
Cyanuric chloride	157	2670
Cyclobutane	115	2601
Cyclobutyl chloroformate	155	2744
1,5,9-Cyclododecatriene	153	2518
Cycloheptane	128	2241
Cycloheptatriene	131	2603
Cycloheptene	128	2242
Cyclohexane	128	1145
Cyclohexanethiol	129	3054
Cyclohexanone	127	1915
Cyclohexene	130	2256
Cyclohexenyltrichlorosilane	156	1762
Cyclohexyl acetate	130	2243
Cyclohexylamine	132	2357
Cyclohexyl isocyanate	155	2488
Cyclohexyl mercaptan	129	3054
Cyclohexyltrichlorosilane	156	1763
Cyclooctadiene phosphines	135	2940
Cyclooctadienes	130P	2520
Cyclooctatetraene	128P	2358
Cyclopentane	128	1146
Cyclopentanol	129	2244
Cyclopentanone	128	2245
Cyclopentene	128	2246
Cyclopropane	115	1027
Cymenes	130	2046
DA	151	——
Dangerous goods in apparatus	171	3363
Dangerous goods in articles	171	3363
Dangerous goods in machinery	171	3363
DC	153	——
Decaborane	134	1868
Decahydronaphthalene	130	1147
n-Decane	128	2247
Denatured alcohol	127	1987
Desensitized explosive, liquid, n.o.s.	113	3379
Desensitized explosive, solid, n.o.s.	113	3380
Deuterium	115	1957
Deuterium, compressed	115	1957
Devices, small, hydrocarbon gas powered, with release device	115	3150
Diacetone alcohol	129	1148
Diacetyl	127	2346
Diallylamine	132	2359
Diallyl ether	131P	2360
4,4'-Diaminodiphenylmethane	153	2651

Name of Material	Guide No.	ID No.
Di-n-amylamine	131	2841
Dibenzyldichlorosilane	156	2434
Diborane	119	1911
Diborane, compressed	119	1911
Diborane mixtures	119	1911
1,2-Dibromobutan-3-one	154	2648
Dibromochloropropanes	159	2872
Dibromodifluoromethane	171	1941
Dibromomethane	160	2664
Di-n-butylamine	132	2248
Dibutylaminoethanol	153	2873
Dibutyl ethers	128	1149
Dichloroacetic acid	153	1764
1,3-Dichloroacetone	153	2649
Dichloroacetyl chloride	156	1765
Dichloroanilines, liquid	153	1590
Dichloroanilines, solid	153	3442
o-Dichlorobenzene	152	1591
2,2'-Dichlorodiethyl ether	152	1916
Dichlorodifluoromethane	126	1028
Dichlorodifluoromethane and Difluoroethane azeotropic mixture with approximately 74% Dichlorodifluoromethane	126	2602
Dichlorodifluoromethane and Ethylene oxide mixture, with not more than 12.5% Ethylene oxide	126	3070
Dichlorodimethyl ether, symmetrical	131	2249
1,1-Dichloroethane	130	2362
1,2-Dichloroethylene	130P	1150
Dichloroethyl ether	152	1916
Dichlorofluoromethane	126	1029
Dichloroisocyanuric acid, dry	140	2465
Dichloroisocyanuric acid salts	140	2465
Dichloroisopropyl ether	153	2490
Dichloromethane	160	1593
1,1-Dichloro-1-nitroethane	153	2650
Dichloropentanes	130	1152
Dichlorophenyl isocyanates	156	2250
Dichlorophenyltrichlorosilane	156	1766
1,2-Dichloropropane	130	1279
1,3-Dichloropropanol-2	153	2750
Dichloropropenes	129	2047
Dichlorosilane	119	2189
1,2-Dichloro-1,1,2,2-tetrafluoroethane	126	1958
3,5-Dichloro-2,4,6-trifluoropyridine	151	9264
Dicyclohexylamine	153	2565
Dicyclohexylammonium nitrite	133	2687
Dicyclopentadiene	130P	2048
1,2-Di-(dimethylamino)ethane	129	2372
Didymium nitrate	140	1465
Diesel fuel	128	1202
Diesel fuel	128	1993
Diethoxymethane	127	2373
3,3-Diethoxypropene	127	2374
Diethylamine	132	1154
2-Diethylaminoethanol	132	2686
3-Diethylaminopropylamine	132	2684
N,N-Diethylaniline	153	2432
Diethylbenzene	130	2049
Diethyl carbonate	128	2366
Diethyldichlorosilane	155	1767
Diethylenetriamine	154	2079

Name of Material	Guide No.	ID No.
Diethyl ether	127	1155
N,N-Diethylethylenediamine	132	2685
Diethyl ketone	127	1156
Diethyl sulfate	152	1594
Diethyl sulfide	129	2375
Diethyl sulphate	152	1594
Diethyl sulphide	129	2375
Diethylthiophosphoryl chloride	155	2751
Diethylzinc	135	1366
Difluorochloroethanes	115	2517
1,1-Difluoroethane	115	1030
Difluoroethane and Dichlorodifluoromethane azeotropic mixture with approximately 74% Dichlorodifluoromethane	126	2602
1,1-Difluoroethylene	116P	1959
Difluoromethane	115	3252
Difluorophosphoric acid, anhydrous	154	1768
2,3-Dihydropyran	127	2376
Diisobutylamine	132	2361
Diisobutylene, isomeric compounds	128	2050
Diisobutyl ketone	128	1157
Diisooctyl acid phosphate	153	1902
Diisopropylamine	132	1158
Diisopropyl ether	127	1159
Diketene, stabilized	131P	2521
1,1-Dimethoxyethane	127	2377
1,2-Dimethoxyethane	127	2252
Dimethylamine, anhydrous	118	1032
Dimethylamine, aqueous solution	132	1160
Dimethylamine, solution	132	1160
2-Dimethylaminoacetonitrile	131	2378
2-Dimethylaminoethanol	132	2051
2-Dimethylaminoethyl acrylate	152	3302
2-Dimethylaminoethyl methacrylate	153P	2522
N,N-Dimethylaniline	153	2253
2,3-Dimethylbutane	128	2457
1,3-Dimethylbutylamine	132	2379
Dimethylcarbamoyl chloride	156	2262
Dimethyl carbonate	129	1161
Dimethylcyclohexanes	128	2263
N,N-Dimethylcyclohexylamine	132	2264
Dimethylcyclohexylamine	132	2264
Dimethyldichlorosilane	155	1162
Dimethyldiethoxysilane	127	2380
Dimethyldioxanes	127	2707
Dimethyl disulfide	131	2381
Dimethyl disulphide	131	2381
Dimethyl ether	115	1033
N,N-Dimethylformamide	129	2265
Dimethylhydrazine, symmetrical	131	2382
Dimethylhydrazine, unsymmetrical	131	1163
2,2-Dimethylpropane	115	2044
Dimethyl-N-propylamine	132	2266
Dimethyl sulfate	156	1595
Dimethyl sulfide	130	1164
Dimethyl sulphate	156	1595
Dimethyl sulphide	130	1164
Dimethyl thiophosphoryl chloride	156	2267
Dimethylzinc	135	1370

Name of Material	Guide No.	ID No.
Dinitroanilines	153	1596
Dinitrobenzenes, liquid	152	1597
Dinitrobenzenes, solid	152	3443
Dinitro-o-cresol	153	1598
Dinitrogen tetroxide	124	1067
Dinitrogen tetroxide and Nitric oxide mixture	124	1975
Dinitrophenol, solution	153	1599
Dinitrophenol, wetted with not less than 15% water	113	1320
Dinitrophenolates, wetted with not less than 15% water	113	1321
Dinitroresorcinol, wetted with not less than 15% water	113	1322
Dinitrotoluenes, liquid	152	2038
Dinitrotoluenes, molten	152	1600
Dinitrotoluenes, solid	152	3454
Dioxane	127	1165
Dioxolane	127	1166
Dipentene	128	2052
Diphenylamine chloroarsine	154	1698
Diphenylchloroarsine, liquid	151	1699
Diphenylchloroarsine, solid	151	3450
Diphenyldichlorosilane	156	1769
Diphenylmethyl bromide	153	1770
Dipicryl sulfide, wetted with not less than 10% water	113	2852
Dipicryl sulphide, wetted with not less than 10% water	113	2852
Dipropylamine	132	2383
Di-n-propyl ether	127	2384
Dipropyl ketone	128	2710
Disinfectant, liquid, corrosive, n.o.s.	153	1903
Disinfectant, liquid, poisonous, n.o.s.	151	3142
Disinfectant, liquid, toxic, n.o.s.	151	3142
Disinfectant, solid, poisonous, n.o.s.	151	1601
Disinfectant, solid, toxic, n.o.s.	151	1601
Disodium trioxosilicate	154	3253
Dispersant gas, n.o.s.	126	1078
Dispersant gases, n.o.s. (flammable)	115	1954
Divinyl ether, stabilized	128P	1167
DM	154	——
Dodecyltrichlorosilane	156	1771
DP	125	——
Dry ice	120	1845
Dye, liquid, corrosive, n.o.s.	154	2801
Dye, liquid, poisonous, n.o.s.	151	1602
Dye, liquid, toxic, n.o.s.	151	1602
Dye, solid, corrosive, n.o.s.	154	3147
Dye, solid, poisonous, n.o.s.	151	3143
Dye, solid, toxic, n.o.s.	151	3143
Dye intermediate, liquid, corrosive, n.o.s.	154	2801
Dye intermediate, liquid, poisonous, n.o.s.	151	1602
Dye intermediate, liquid, toxic, n.o.s.	151	1602
Dye intermediate, solid, corrosive, n.o.s.	154	3147
Dye intermediate, solid, poisonous, n.o.s.	151	3143
Dye intermediate, solid, toxic, n.o.s.	151	3143
ED	151	——

Name of Material	Guide No.	ID No.
Elevated temperature liquid, flammable, n.o.s., with flash point above 37.8°C (100°F), at or above its flash point	**128**	3256
Elevated temperature liquid, flammable, n.o.s., with flash point above 60°C (140°F), at or above its flash point	**128**	3256
Elevated temperature liquid, n.o.s., at or above 100°C (212°F), and below its flash point	**171**	3257
Elevated temperature solid, n.o.s., at or above 240°C (464°F)	**171**	3258
Engine, fuel cell, flammable gas powered	**115**	3166
Engine, fuel cell, flammable gas powered	**115**	3529
Engine, fuel cell, flammable liquid powered	**128**	3166
Engine, fuel cell, flammable liquid powered	**128**	3528
Engine, internal combustion	**128**	3166
Engine, internal combustion	**171**	3530
Engine, internal combustion, flammable gas powered	**115**	3529
Engine, internal combustion, flammable liquid powered	**128**	3528
Engines, internal combustion, flammable gas powered	**115**	3166
Engines, internal combustion, flammable liquid powered	**128**	3166
Environmentally hazardous substance, liquid, n.o.s.	**171**	3082
Environmentally hazardous substance, solid, n.o.s.	**171**	3077
Epibromohydrin	**131**	2558
Epichlorohydrin	**131P**	2023
1,2-Epoxy-3-ethoxypropane	**127**	2752
Esters, n.o.s.	**127**	3272
Ethane	**115**	1035
Ethane, compressed	**115**	1035
Ethane, refrigerated liquid	**115**	1961
Ethane-Propane mixture, refrigerated liquid	**115**	1961
Ethanol	**127**	1170
Ethanol and gasoline mixture, with more than 10% ethanol	**127**	3475
Ethanol and motor spirit mixture, with more than 10% ethanol	**127**	3475
Ethanol and petrol mixture, with more than 10% ethanol	**127**	3475
Ethanol, solution	**127**	1170
Ethanolamine	**153**	2491
Ethanolamine, solution	**153**	2491
Ethers, n.o.s.	**127**	3271
Ethyl acetate	**129**	1173
Ethylacetylene, stabilized	**116P**	2452
Ethyl acrylate, stabilized	**129P**	1917
Ethyl alcohol	**127**	1170
Ethyl alcohol, solution	**127**	1170
Ethylamine	**118**	1036
Ethylamine, aqueous solution, with not less than 50% but not more than 70% Ethylamine	**132**	2270
Ethyl amyl ketone	**128**	2271
2-Ethylaniline	**153**	2273
N-Ethylaniline	**153**	2272
Ethylbenzene	**130**	1175
N-Ethyl-N-benzylaniline	**153**	2274
N-Ethylbenzyltoluidines, liquid	**153**	2753
N-Ethylbenzyltoluidines, solid	**153**	3460

Name of Material	Guide No.	ID No.
Ethyl borate	129	1176
Ethyl bromide	131	1891
Ethyl bromoacetate	155	1603
2-Ethylbutanol	129	2275
2-Ethylbutyl acetate	130	1177
Ethyl butyl ether	127	1179
2-Ethylbutyraldehyde	130	1178
Ethyl butyrate	130	1180
Ethyl chloride	115	1037
Ethyl chloroacetate	155	1181
Ethyl chloroformate	155	1182
Ethyl 2-chloropropionate	129	2935
Ethyl chlorothioformate	155	2826
Ethyl crotonate	130	1862
Ethyldichloroarsine	151	1892
Ethyldichlorosilane	139	1183
Ethylene	116P	1962
Ethylene, Acetylene and Propylene in mixture, refrigerated liquid containing at least 71.5% Ethylene with not more than 22.5% Acetylene and not more than 6% Propylene	115	3138
Ethylene, compressed	116P	1962
Ethylene, refrigerated liquid (cryogenic liquid)	115	1038
Ethylene chlorohydrin	131	1135
Ethylenediamine	132	1604
Ethylene dibromide	154	1605
Ethylene dibromide and Methyl bromide mixture, liquid	151	1647
Ethylene dichloride	131	1184
Ethylene glycol diethyl ether	127	1153
Ethylene glycol monoethyl ether	127	1171
Ethylene glycol monoethyl ether acetate	129	1172
Ethylene glycol monomethyl ether	127	1188
Ethylene glycol monomethyl ether acetate	129	1189
Ethyleneimine, stabilized	131P	1185
Ethylene oxide	119P	1040
Ethylene oxide and Carbon dioxide mixture, with more than 9% but not more than 87% Ethylene oxide	115	1041
Ethylene oxide and Carbon dioxide mixture, with more than 87% Ethylene oxide	119P	3300
Ethylene oxide and Carbon dioxide mixtures, with not more than 9% Ethylene oxide	126	1952
Ethylene oxide and Chlorotetrafluoroethane mixture, with not more than 8.8% Ethylene oxide	126	3297
Ethylene oxide and Dichlorodifluoromethane mixture, with not more than 12.5% Ethylene oxide	126	3070
Ethylene oxide and Pentafluoroethane mixture, with not more than 7.9% Ethylene oxide	126	3298
Ethylene oxide and Propylene oxide mixture, with not more than 30% Ethylene oxide	131P	2983
Ethylene oxide and Tetrafluoroethane mixture, with not more than 5.6% Ethylene oxide	126	3299
Ethylene oxide with Nitrogen	119P	1040
Ethyl ether	127	1155
Ethyl fluoride	115	2453

Name of Material	Guide No.	ID No.
Ethyl formate	129	1190
Ethylhexaldehydes	129	1191
2-Ethylhexylamine	132	2276
2-Ethylhexyl chloroformate	156	2748
Ethyl isobutyrate	129	2385
Ethyl isocyanate	155	2481
Ethyl lactate	129	1192
Ethyl mercaptan	129	2363
Ethyl methacrylate, stabilized	130P	2277
Ethyl methyl ether	115	1039
Ethyl methyl ketone	127	1193
Ethyl nitrite, solution	131	1194
Ethyl orthoformate	129	2524
Ethyl oxalate	156	2525
Ethylphenyldichlorosilane	156	2435
Ethyl phosphonothioic dichloride, anhydrous	154	2927
Ethyl phosphonous dichloride, anhydrous	135	2845
Ethyl phosphorodichloridate	154	2927
1-Ethylpiperidine	132	2386
Ethyl propionate	129	1195
Ethyl propyl ether	127	2615
Ethyl silicate	129	1292
N-Ethyltoluidines	153	2754
Ethyltrichlorosilane	155	1196
Explosives, division 1.1, 1.2, 1.3 or 1.5	112	——
Explosives, division 1.4 or 1.6	114	——
Extracts, aromatic, liquid	127	1169
Extracts, flavoring, liquid	127	1197
Extracts, flavouring, liquid	127	1197
Fabrics, animal or vegetable or synthetic, n.o.s. with oil	133	1373
Fabrics impregnated with weakly nitrated Nitrocellulose, n.o.s.	133	1353
Ferric arsenate	151	1606
Ferric arsenite	151	1607
Ferric chloride, anhydrous	157	1773
Ferric chloride, solution	154	2582
Ferric nitrate	140	1466
Ferrocerium	170	1323
Ferrosilicon	139	1408
Ferrous arsenate	151	1608
Ferrous chloride, solid	154	1759
Ferrous chloride, solution	154	1760
Ferrous metal borings, shavings, turnings or cuttings	170	2793
Fertilizer, ammoniating solution, with free Ammonia	125	1043
Fibers, animal or vegetable, burnt, wet or damp	133	1372
Fibers, animal or vegetable or synthetic, n.o.s. with oil	133	1373
Fibers, vegetable, dry	133	3360
Fibers impregnated with weakly nitrated Nitrocellulose, n.o.s.	133	1353
Fibres, animal or vegetable, burnt, wet or damp	133	1372
Fibres, animal or vegetable or synthetic, n.o.s. with oil	133	1373
Fibres, vegetable, dry	133	3360
Fibres impregnated with weakly nitrated Nitrocellulose, n.o.s.	133	1353
Films, nitrocellulose base	133	1324
Fire extinguisher charges, corrosive liquid	154	1774

Name of Material	Guide No.	ID No.
Fire extinguishers with compressed or liquefied gas	126	1044
Firelighters, solid, with flammable liquid	133	2623
First aid kit	171	3316
Fish meal, stabilized	171	2216
Fish meal, unstabilized	133	1374
Fish scrap, stabilized	171	2216
Fish scrap, unstabilized	133	1374
Flammable liquid, corrosive, n.o.s	132	2924
Flammable liquid, n.o.s.	128	1993
Flammable liquid, poisonous, corrosive, n.o.s.	131	3286
Flammable liquid, poisonous, n.o.s.	131	1992
Flammable liquid, toxic, corrosive, n.o.s.	131	3286
Flammable liquid, toxic, n.o.s.	131	1992
Flammable solid, corrosive, inorganic, n.o.s.	134	3180
Flammable solid, corrosive, organic, n.o.s.	134	2925
Flammable solid, inorganic, n.o.s.	133	3178
Flammable solid, organic, molten, n.o.s.	133	3176
Flammable solid, organic, n.o.s.	133	1325
Flammable solid, oxidizing, n.o.s.	140	3097
Flammable solid, poisonous, inorganic, n.o.s.	134	3179
Flammable solid, poisonous, organic, n.o.s.	134	2926
Flammable solid, toxic, inorganic, n.o.s.	134	3179
Flammable solid, toxic, organic, n.o.s.	134	2926
Fluorine	124	1045
Fluorine, compressed	124	1045
Fluoroacetic acid	154	2642
Fluoroanilines	153	2941
Fluorobenzene	130	2387
Fluoroboric acid	154	1775
Fluorophosphoric acid, anhydrous	154	1776
Fluorosilicates, n.o.s.	151	2856
Fluorosilicic acid	154	1778
Fluorosulfonic acid	137	1777
Fluorosulphonic acid	137	1777
Fluorotoluenes	130	2388
Formaldehyde, solution (corrosive)	153	2209
Formaldehyde, solution, flammable	132	1198
Formalin (corrosive)	153	2209
Formalin (flammable)	132	1198
Formic acid	153	1779
Formic acid, with more than 85% acid	153	1779
Formic acid, with not less than 5% but less than 10% acid	153	3412
Formic acid, with not less than 10% but not more than 85% acid	153	3412
Fuel, aviation, turbine engine	128	1863
Fuel cell cartridges, containing corrosive substances	153	3477
Fuel cell cartridges, containing flammable liquids	128	3473
Fuel cell cartridges, containing hydrogen in metal hydride	115	3479

Name of Material	Guide No.	ID No.
Fuel cell cartridges, containing liquefied flammable gas	115	3478
Fuel cell cartridges, containing water-reactive substances	138	3476
Fuel cell cartridges contained in equipment, containing corrosive substances	153	3477
Fuel cell cartridges contained in equipment, containing flammable liquids	128	3473
Fuel cell cartridges contained in equipment, containing hydrogen in metal hydride	115	3479
Fuel cell cartridges contained in equipment, containing liquefied flammable gas	115	3478
Fuel cell cartridges contained in equipment, containing water-reactive substances	138	3476
Fuel cell cartridges packed with equipment, containing corrosive substances	153	3477
Fuel cell cartridges packed with equipment, containing flammable liquids	128	3473
Fuel cell cartridges packed with equipment, containing hydrogen in metal hydride	115	3479
Fuel cell cartridges packed with equipment, containing liquefied flammable gas	115	3478
Fuel cell cartridges packed with equipment, containing water-reactive substances	138	3476
Fuel oil	128	1202
Fuel oil	128	1993
Fumaryl chloride	156	1780
Fumigated cargo transport unit	171	3359
Furaldehydes	153P	1199
Furan	128	2389
Furfuryl alcohol	153	2874
Furfurylamine	132	2526
Fusee (railway or highway)	133	1325
Fusel oil	127	1201
GA	153	——
Gallium	172	2803
Gas, refrigerated liquid, flammable, n.o.s.	115	3312
Gas, refrigerated liquid, n.o.s.	120	3158
Gas, refrigerated liquid, oxidizing, n.o.s.	122	3311
Gas cartridges	115	2037
Gas identification set	123	9035
Gasohol	128	1203
Gas oil	128	1202
Gasoline	128	1203
Gasoline and ethanol mixture, with more than 10% ethanol	127	3475
Gas sample, non-pressurized, flammable, n.o.s., not refrigerated liquid	115	3167
Gas sample, non-pressurized, poisonous, flammable, n.o.s., not refrigerated liquid	119	3168
Gas sample, non-pressurized, poisonous, n.o.s., not refrigerated liquid	123	3169
Gas sample, non-pressurized, toxic, flammable, n.o.s., not refrigerated liquid	119	3168
Gas sample, non-pressurized, toxic, n.o.s., not refrigerated liquid	123	3169
GB	153	——
GD	153	——
Genetically modified micro-organisms	171	3245
Genetically modified organisms	171	3245

Name of Material	Guide No.	ID No.
Germane	119	2192
Germane, adsorbed	173	3523
GF	153	——
Glycerol alpha-monochlorohydrin	153	2689
Glycidaldehyde	131P	2622
Guanidine nitrate	143	1467
H	153	——
Hafnium powder, dry	135	2545
Hafnium powder, wetted with not less than 25% water	170	1326
Halogenated monomethyldiphenylmethanes, liquid	171	3151
Halogenated monomethyldiphenylmethanes, solid	171	3152
Hay, wet, damp or contaminated with oil	133	1327
Hazardous waste, liquid, n.o.s.	171	3082
Hazardous waste, solid, n.o.s.	171	3077
HD	153	——
Heating oil, light	128	1202
Helium	120	1046
Helium, compressed	120	1046
Helium, refrigerated liquid (cryogenic liquid)	120	1963
Heptafluoropropane	126	3296
n-Heptaldehyde	129	3056
Heptanes	128	1206
n-Heptene	128	2278
Hexachloroacetone	153	2661
Hexachlorobenzene	152	2729
Hexachlorobutadiene	151	2279
Hexachlorocyclopentadiene	151	2646
Hexachlorophene	151	2875
Hexadecyltrichlorosilane	156	1781
Hexadiene	130	2458
Hexaethyl tetraphosphate	151	1611
Hexaethyl tetraphosphate and compressed gas mixture	123	1612
Hexafluoroacetone	125	2420
Hexafluoroacetone hydrate, liquid	151	2552
Hexafluoroacetone hydrate, solid	151	3436
Hexafluoroethane	126	2193
Hexafluoroethane, compressed	126	2193
Hexafluorophosphoric acid	154	1782
Hexafluoropropylene	126	1858
Hexafluoropropylene, compressed	126	1858
Hexaldehyde	130	1207
Hexamethylenediamine, solid	153	2280
Hexamethylenediamine, solution	153	1783
Hexamethylene diisocyanate	156	2281
Hexamethyleneimine	132	2493
Hexamethylenetetramine	133	1328
Hexanes	128	1208
Hexanoic acid	153	2829
Hexanols	129	2282
1-Hexene	128	2370
Hexyltrichlorosilane	156	1784
HL	153	——
HN-1	153	——
HN-2	153	——
HN-3	153	——
Hydrazine, anhydrous	132	2029

Name of Material	Guide No.	ID No.
Hydrazine aqueous solution, flammable, with more than 37% hydrazine, by mass	132	3484
Hydrazine, aqueous solution, with more than 37% Hydrazine	153	2030
Hydrazine, aqueous solution, with not more than 37% Hydrazine	152	3293
Hydriodic acid	154	1787
Hydrobromic acid	154	1788
Hydrocarbon and butadienes mixture, stabilized	116P	1010
Hydrocarbon gas mixture, compressed, n.o.s.	115	1964
Hydrocarbon gas mixture, liquefied, n.o.s.	115	1965
Hydrocarbon gas refills for small devices, with release device	115	3150
Hydrocarbons, liquid, n.o.s.	128	3295
Hydrochloric acid	157	1789
Hydrocyanic acid, aqueous solution, with less than 5% Hydrogen cyanide	154	1613
Hydrocyanic acid, aqueous solution, with not more than 20% Hydrogen cyanide	154	1613
Hydrofluoric acid	157	1790
Hydrofluoric acid and Sulfuric acid mixture	157	1786
Hydrofluoric acid and Sulphuric acid mixture	157	1786
Hydrofluorosilicic acid	154	1778
Hydrogen	115	1049
Hydrogen, compressed	115	1049
Hydrogen in a metal hydride storage system	115	3468
Hydrogen in a metal hydride storage system contained in equipment	115	3468
Hydrogen in a metal hydride storage system packed with equipment	115	3468
Hydrogen, refrigerated liquid (cryogenic liquid)	115	1966
Hydrogen and Methane mixture, compressed	115	2034
Hydrogen bromide, anhydrous	125	1048
Hydrogen chloride, anhydrous	125	1050
Hydrogen chloride, refrigerated liquid	125	2186
Hydrogen cyanide, anhydrous, stabilized	117P	1051
Hydrogen cyanide, aqueous solution, with not more than 20% Hydrogen cyanide	154	1613
Hydrogen cyanide, solution in alcohol, with not more than 45% Hydrogen cyanide	131	3294
Hydrogen cyanide, stabilized	117P	1051
Hydrogen cyanide, stabilized (absorbed)	152	1614
Hydrogendifluorides, solid, n.o.s.	154	1740
Hydrogendifluorides, solution, n.o.s.	154	3471
Hydrogen fluoride, anhydrous	125	1052
Hydrogen iodide, anhydrous	125	2197
Hydrogen peroxide, aqueous solution, stabilized, with more than 60% Hydrogen peroxide	143	2015
Hydrogen peroxide, aqueous solution, with not less than 8% but less than 20% Hydrogen peroxide	140	2984

Name of Material	Guide No.	ID No.
Hydrogen peroxide, aqueous solution, with not less than 20% but not more than 60% Hydrogen peroxide (stabilized as necessary)	140	2014
Hydrogen peroxide, stabilized	143	2015
Hydrogen peroxide and Peroxyacetic acid mixture, with acid(s), water and not more than 5% Peroxyacetic acid, stabilized	140	3149
Hydrogen selenide, adsorbed	173	3526
Hydrogen selenide, anhydrous	117	2202
Hydrogen sulfide	117	1053
Hydrogen sulphide	117	1053
1-Hydroxybenzotriazole, anhydrous, wetted with not less than 20% water	113	3474
1-Hydroxybenzotriazole, monohydrate	113	3474
Hydroxylamine sulfate	154	2865
Hydroxylamine sulphate	154	2865
Hypochlorite solution	154	1791
Hypochlorites, inorganic, n.o.s.	140	3212
3,3'-Iminodipropylamine	153	2269
Infectious substance, affecting animals only	158	2900
Infectious substance, affecting humans	158	2814
Ink, printer's, flammable	129	1210
Insecticide gas, flammable, n.o.s.	115	3354
Insecticide gas, n.o.s.	126	1968
Insecticide gas, poisonous, flammable, n.o.s.	119	3355
Insecticide gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone A)	119	3355
Insecticide gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone B)	119	3355
Insecticide gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone C)	119	3355
Insecticide gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone D)	119	3355
Insecticide gas, poisonous, n.o.s.	123	1967
Insecticide gas, toxic, flammable, n.o.s.	119	3355
Insecticide gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone A)	119	3355
Insecticide gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone B)	119	3355
Insecticide gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone C)	119	3355
Insecticide gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone D)	119	3355
Insecticide gas, toxic, n.o.s.	123	1967
Iodine	154	3495
Iodine monochloride, liquid	157	3498
Iodine monochloride, solid	157	1792
Iodine pentafluoride	144	2495
2-Iodobutane	129	2390
Iodomethylpropanes	129	2391
Iodopropanes	129	2392
Iron oxide, spent	135	1376
Iron pentacarbonyl	136	1994
Iron sponge, spent	135	1376
Isobutane	115	1075
Isobutane	115	1969

Name of Material	Guide No.	ID No.
Isobutanol	129	1212
Isobutyl acetate	129	1213
Isobutyl acrylate, stabilized	129P	2527
Isobutyl alcohol	129	1212
Isobutyl aldehyde	130	2045
Isobutylamine	132	1214
Isobutyl chloroformate	155	2742
Isobutylene	115	1055
Isobutylene	115	1075
Isobutyl formate	129	2393
Isobutyl isobutyrate	130	2528
Isobutyl isocyanate	155P	2486
Isobutyl methacrylate, stabilized	130P	2283
Isobutyl propionate	129	2394
Isobutyraldehyde	130	2045
Isobutyric acid	132	2529
Isobutyronitrile	131	2284
Isobutyryl chloride	132	2395
Isocyanate solution, flammable, poisonous, n.o.s.	155	2478
Isocyanate solution, flammable, toxic, n.o.s.	155	2478
Isocyanate solution, poisonous, flammable, n.o.s.	155	3080
Isocyanate solution, poisonous, n.o.s.	155	2206
Isocyanate solution, toxic, flammable, n.o.s.	155	3080
Isocyanate solution, toxic, n.o.s.	155	2206
Isocyanates, flammable, poisonous, n.o.s.	155	2478
Isocyanates, flammable, toxic, n.o.s.	155	2478
Isocyanates, poisonous, flammable, n.o.s.	155	3080
Isocyanates, poisonous, n.o.s.	155	2206
Isocyanates, toxic, flammable, n.o.s.	155	3080
Isocyanates, toxic, n.o.s.	155	2206
Isocyanatobenzotrifluorides	156	2285
Isoheptenes	128	2287
Isohexenes	128	2288
Isooctane	128	1262
Isooctenes	128	1216
Isopentane	128	1265
Isopentenes	128	2371
Isophoronediamine	153	2289
Isophorone diisocyanate	156	2290
Isoprene, stabilized	130P	1218
Isopropanol	129	1219
Isopropenyl acetate	129P	2403
Isopropenylbenzene	128	2303
Isopropyl acetate	129	1220
Isopropyl acid phosphate	153	1793
Isopropyl alcohol	129	1219
Isopropylamine	132	1221
Isopropylbenzene	130	1918
Isopropyl butyrate	129	2405
Isopropyl chloroacetate	155	2947
Isopropyl chloroformate	155	2407
Isopropyl 2-chloropropionate	129	2934
Isopropyl isobutyrate	127	2406
Isopropyl isocyanate	155P	2483
Isopropyl nitrate	130	1222
Isopropyl propionate	129	2409
Isosorbide dinitrate mixture	133	2907

Name of Material	Guide No.	ID No.
Isosorbide-5-mononitrate	133	3251
Kerosene	128	1223
Ketones, liquid, n.o.s.	127	1224
Krill meal	133	3497
Krypton	120	1056
Krypton, compressed	120	1056
Krypton, refrigerated liquid (cryogenic liquid)	120	1970
L (Lewisite)	153	——
Lead acetate	151	1616
Lead arsenates	151	1617
Lead arsenites	151	1618
Lead compound, soluble, n.o.s.	151	2291
Lead cyanide	151	1620
Lead dioxide	140	1872
Lead nitrate	141	1469
Lead perchlorate, solid	141	1470
Lead perchlorate, solution	141	3408
Lead phosphite, dibasic	133	2989
Lead sulfate, with more than 3% free acid	154	1794
Lead sulphate, with more than 3% free acid	154	1794
Lewisite	153	——
Life-saving appliances, not self-inflating	171	3072
Life-saving appliances, self-inflating	171	2990
Lighter refills containing flammable gas	115	1057
Lighters containing flammable gas	115	1057
Lighters, non-pressurized, containing flammable liquid	128	1057
Liquefied gas, flammable, n.o.s.	115	3161
Liquefied gas, n.o.s.	126	3163
Liquefied gas, oxidizing, n.o.s.	122	3157
Liquefied gas, poisonous, corrosive, n.o.s.	125	3308
Liquefied gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone A)	125	3308
Liquefied gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone B)	125	3308
Liquefied gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone C)	125	3308
Liquefied gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone D)	125	3308
Liquefied gas, poisonous, flammable, corrosive, n.o.s.	119	3309
Liquefied gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)	119	3309
Liquefied gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)	119	3309
Liquefied gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone C)	119	3309
Liquefied gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone D)	119	3309
Liquefied gas, poisonous, flammable, n.o.s.	119	3160
Liquefied gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone A)	119	3160
Liquefied gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone B)	119	3160

Name of Material	Guide No.	ID No.
Liquefied gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone C)	119	3160
Liquefied gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone D)	119	3160
Liquefied gas, poisonous, n.o.s.	123	3162
Liquefied gas, poisonous, n.o.s. (Inhalation Hazard Zone A)	123	3162
Liquefied gas, poisonous, n.o.s. (Inhalation Hazard Zone B)	123	3162
Liquefied gas, poisonous, n.o.s. (Inhalation Hazard Zone C)	123	3162
Liquefied gas, poisonous, n.o.s. (Inhalation Hazard Zone D)	123	3162
Liquefied gas, poisonous, oxidizing, corrosive, n.o.s.	124	3310
Liquefied gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone A)	124	3310
Liquefied gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone B)	124	3310
Liquefied gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone C)	124	3310
Liquefied gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone D)	124	3310
Liquefied gas, poisonous, oxidizing, n.o.s.	124	3307
Liquefied gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone A)	124	3307
Liquefied gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone B)	124	3307
Liquefied gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone C)	124	3307
Liquefied gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone D)	124	3307
Liquefied gas, toxic, corrosive, n.o.s.	125	3308
Liquefied gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone A)	125	3308
Liquefied gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone B)	125	3308
Liquefied gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone C)	125	3308
Liquefied gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone D)	125	3308
Liquefied gas, toxic, flammable, corrosive, n.o.s.	119	3309
Liquefied gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)	119	3309
Liquefied gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)	119	3309
Liquefied gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone C)	119	3309
Liquefied gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone D)	119	3309
Liquefied gas, toxic, flammable, n.o.s.	119	3160
Liquefied gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone A)	119	3160
Liquefied gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone B)	119	3160

Name of Material	Guide No.	ID No.
Liquefied gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone C)	119	3160
Liquefied gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone D)	119	3160
Liquefied gas, toxic, n.o.s.	123	3162
Liquefied gas, toxic, n.o.s. (Inhalation Hazard Zone A)	123	3162
Liquefied gas, toxic, n.o.s. (Inhalation Hazard Zone B)	123	3162
Liquefied gas, toxic, n.o.s. (Inhalation Hazard Zone C)	123	3162
Liquefied gas, toxic, n.o.s. (Inhalation Hazard Zone D)	123	3162
Liquefied gas, toxic, oxidizing, corrosive, n.o.s.	124	3310
Liquefied gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone A)	124	3310
Liquefied gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone B)	124	3310
Liquefied gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone C)	124	3310
Liquefied gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone D)	124	3310
Liquefied gas, toxic, oxidizing, n.o.s.	124	3307
Liquefied gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone A)	124	3307
Liquefied gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone B)	124	3307
Liquefied gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone C)	124	3307
Liquefied gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone D)	124	3307
Liquefied gases, non-flammable, charged with Nitrogen, Carbon dioxide or Air	120	1058
Liquefied natural gas (cryogenic liquid)	115	1972
Liquefied petroleum gas	115	1075
Lithium	138	1415
Lithium aluminum hydride	138	1410
Lithium aluminum hydride, ethereal	138	1411
Lithium batteries	138	3090
Lithium batteries contained in equipment	138	3091
Lithium batteries installed in cargo transport unit (lithium ion batteries)	147	3536
Lithium batteries installed in cargo transport unit (lithium metal batteries)	138	3536
Lithium batteries packed with equipment	138	3091
Lithium borohydride	138	1413
Lithium ferrosilicon	139	2830
Lithium hydride	138	1414
Lithium hydride, fused solid	138	2805
Lithium hydroxide	154	2680
Lithium hydroxide, solution	154	2679
Lithium hypochlorite, dry	140	1471
Lithium hypochlorite mixture	140	1471
Lithium hypochlorite mixtures, dry	140	1471
Lithium ion batteries (including lithium ion polymer batteries)	147	3480

Name of Material	Guide No.	ID No.
Lithium ion batteries contained in equipment (including lithium ion polymer batteries)	147	3481
Lithium ion batteries packed with equipment (including lithium ion polymer batteries)	147	3481
Lithium metal batteries (including lithium alloy batteries)	138	3090
Lithium metal batteries contained in equipment (including lithium alloy batteries)	138	3091
Lithium metal batteries packed with equipment (including lithium alloy batteries)	138	3091
Lithium nitrate	140	2722
Lithium nitride	139	2806
Lithium peroxide	143	1472
Lithium silicon	138	1417
LNG (cryogenic liquid)	115	1972
London purple	151	1621
LPG	115	1075
Machinery, fuel cell, flammable gas powered	115	3529
Machinery, fuel cell, flammable liquid powered	128	3528
Machinery, internal combustion	171	3530
Machinery, internal combustion, flammable gas powered	115	3529
Machinery, internal combustion, flammable liquid powered	128	3528
Magnesium	138	1869
Magnesium, in pellets, turnings or ribbons	138	1869
Magnesium alkyls	135	3053
Magnesium alloys, with more than 50% Magnesium, in pellets, turnings or ribbons	138	1869
Magnesium alloys powder	138	1418
Magnesium aluminum phosphide	139	1419
Magnesium arsenate	151	1622
Magnesium bromate	140	1473
Magnesium chlorate	140	2723
Magnesium chloride and Chlorate mixture, solid	140	1459
Magnesium chloride and Chlorate mixture, solution	140	3407
Magnesium diamide	135	2004
Magnesium diphenyl	135	2005
Magnesium fluorosilicate	151	2853
Magnesium granules, coated	138	2950
Magnesium hydride	138	2010
Magnesium nitrate	140	1474
Magnesium perchlorate	140	1475
Magnesium peroxide	140	1476
Magnesium phosphide	139	2011
Magnesium powder	138	1418
Magnesium silicide	138	2624
Magnetized material	171	2807
Maleic anhydride	156	2215
Maleic anhydride, molten	156	2215
Malononitrile	153	2647
Maneb	135	2210
Maneb, stabilized	135	2968
Maneb preparation, stabilized	135	2968
Maneb preparation, with not less than 60% Maneb	135	2210
Manganese nitrate	140	2724

Name of Material	Guide No.	ID No.
Manganese resinate	133	1330
Matches, fusee	133	2254
Matches, safety	133	1944
Matches, "strike anywhere"	133	1331
Matches, wax "vesta"	133	1945
MD	152	——
Medical waste, category A, affecting animals only, solid	158	3549
Medical waste, category A, affecting humans, solid	158	3549
Medical waste, n.o.s.	158	3291
Medicine, liquid, flammable, poisonous, n.o.s.	131	3248
Medicine, liquid, flammable, toxic, n.o.s.	131	3248
Medicine, liquid, poisonous, n.o.s.	151	1851
Medicine, liquid, toxic, n.o.s.	151	1851
Medicine, solid, poisonous, n.o.s.	151	3249
Medicine, solid, toxic, n.o.s.	151	3249
Mercaptan mixture, liquid, flammable, n.o.s.	130	3336
Mercaptan mixture, liquid, flammable, poisonous, n.o.s.	131	1228
Mercaptan mixture, liquid, flammable, toxic, n.o.s.	131	1228
Mercaptan mixture, liquid, poisonous, flammable, n.o.s.	131	3071
Mercaptan mixture, liquid, toxic, flammable, n.o.s.	131	3071
Mercaptans, liquid, flammable, n.o.s.	130	3336
Mercaptans, liquid, flammable, poisonous, n.o.s.	131	1228
Mercaptans, liquid, flammable, toxic, n.o.s.	131	1228
Mercaptans, liquid, poisonous, flammable, n.o.s.	131	3071
Mercaptans, liquid, toxic, flammable, n.o.s.	131	3071
Mercuric arsenate	151	1623
Mercuric chloride	154	1624
Mercuric nitrate	141	1625
Mercuric potassium cyanide	157	1626
Mercurous nitrate	141	1627
Mercury	172	2809
Mercury acetate	151	1629
Mercury ammonium chloride	151	1630
Mercury based pesticide, liquid, flammable, poisonous	131	2778
Mercury based pesticide, liquid, flammable, toxic	131	2778
Mercury based pesticide, liquid, poisonous	151	3012
Mercury based pesticide, liquid, poisonous, flammable	131	3011
Mercury based pesticide, liquid, toxic	151	3012
Mercury based pesticide, liquid, toxic, flammable	131	3011
Mercury based pesticide, solid, poisonous	151	2777
Mercury based pesticide, solid, toxic	151	2777
Mercury benzoate	154	1631
Mercury bromides	154	1634
Mercury compound, liquid, n.o.s.	151	2024
Mercury compound, solid, n.o.s.	151	2025
Mercury contained in manufactured articles	172	3506
Mercury cyanide	154	1636

Name of Material	Guide No.	ID No.
Mercury gluconate	151	1637
Mercury iodide	151	1638
Mercury nucleate	151	1639
Mercury oleate	151	1640
Mercury oxide	151	1641
Mercury oxycyanide, desensitized	151	1642
Mercury potassium iodide	151	1643
Mercury salicylate	151	1644
Mercury sulfate	151	1645
Mercury sulphate	151	1645
Mercury thiocyanate	151	1646
Mesityl oxide	129	1229
Metal carbonyls, liquid, n.o.s.	151	3281
Metal carbonyls, solid, n.o.s.	151	3466
Metal catalyst, dry	135	2881
Metal catalyst, wetted	170	1378
Metaldehyde	133	1332
Metal hydrides, flammable, n.o.s.	170	3182
Metal hydrides, water-reactive, n.o.s.	138	1409
Metallic substance, water-reactive, n.o.s.	138	3208
Metallic substance, water-reactive, self-heating, n.o.s.	138	3209
Metal powder, flammable, n.o.s.	170	3089
Metal powder, self-heating, n.o.s.	135	3189
Metal salts of organic compounds, flammable, n.o.s.	133	3181
Methacrylaldehyde, stabilized	131P	2396
Methacrylic acid, stabilized	153P	2531
Methacrylonitrile, stabilized	131P	3079
Methallyl alcohol	129	2614
Methane	115	1971
Methane, compressed	115	1971
Methane, refrigerated liquid (cryogenic liquid)	115	1972
Methane and Hydrogen mixture, compressed	115	2034
Methanesulfonyl chloride	156	3246
Methanesulphonyl chloride	156	3246
Methanol	131	1230
Methoxymethyl isocyanate	155	2605
4-Methoxy-4-methylpentan-2-one	128	2293
1-Methoxy-2-propanol	129	3092
Methyl acetate	129	1231
Methylacetylene and Propadiene mixture, stabilized	116P	1060
Methyl acrylate, stabilized	129P	1919
Methylal	127	1234
Methyl alcohol	131	1230
Methylallyl chloride	130P	2554
Methylamine, anhydrous	118	1061
Methylamine, aqueous solution	132	1235
Methylamyl acetate	130	1233
Methylamyl alcohol	129	2053
Methyl amyl ketone	127	1110
N-Methylaniline	153	2294
Methylbenzyl (alpha) alcohol, liquid	153	2937
Methylbenzyl (alpha) alcohol, solid	153	3438
Methyl bromide	123	1062

Name of Material	Guide No.	ID No.
Methyl bromide and Chloropicrin mixture	123	1581
Methyl bromide and Ethylene dibromide mixture, liquid	151	1647
Methyl bromoacetate	155	2643
2-Methylbutanal	129	3371
3-Methylbutan-2-one	127	2397
2-Methyl-1-butene	128	2459
2-Methyl-2-butene	128	2460
3-Methyl-1-butene	128	2561
N-Methylbutylamine	132	2945
Methyl tert-butyl ether	127	2398
Methyl butyrate	129	1237
Methyl chloride	115	1063
Methyl chloride and Chloropicrin mixture	119	1582
Methyl chloride and Methylene chloride mixture	115	1912
Methyl chloroacetate	155	2295
Methyl chloroformate	155	1238
Methyl chloromethyl ether	131	1239
Methyl 2-chloropropionate	129	2933
Methylchlorosilane	119	2534
Methylcyclohexane	128	2296
Methylcyclohexanols	129	2617
Methylcyclohexanone	128	2297
Methylcyclopentane	128	2298
Methyl dichloroacetate	155	2299
Methyldichloroarsine	152	1556
Methyldichlorosilane	139	1242
Methylene chloride	160	1593
Methylene chloride and Methyl chloride mixture	115	1912
Methyl ethyl ether	115	1039
Methyl ethyl ketone	127	1193
2-Methyl-5-ethylpyridine	153	2300
Methyl fluoride	115	2454
Methyl formate	129	1243
2-Methylfuran	128	2301
2-Methyl-2-heptanethiol	131	3023
5-Methylhexan-2-one	127	2302
Methylhydrazine	131	1244
Methyl iodide	151	2644
Methyl isobutyl carbinol	129	2053
Methyl isobutyl ketone	127	1245
Methyl isocyanate	155P	2480
Methyl isopropenyl ketone, stabilized	127P	1246
Methyl isothiocyanate	131	2477
Methyl isovalerate	130	2400
Methyl magnesium bromide in Ethyl ether	138	1928
Methyl mercaptan	117	1064
Methyl methacrylate monomer, stabilized	129P	1247
4-Methylmorpholine	132	2535
N-Methylmorpholine	132	2535
Methyl nitrite	116	2455
Methyl orthosilicate	155	2606
Methylpentadiene	128	2461
2-Methylpentan-2-ol	129	2560
Methylphenyldichlorosilane	156	2437
Methyl phosphonic dichloride	137	9206
Methyl phosphonous dichloride	135	2845
1-Methylpiperidine	132	2399
Methyl propionate	129	1248
Methyl propyl ether	127	2612

Name of Material	Guide No.	ID No.
Methyl propyl ketone	127	1249
Methyltetrahydrofuran	127	2536
Methyl trichloroacetate	156	2533
Methyltrichlorosilane	155	1250
Methyl valeraldehyde (alpha)	130	2367
Methyl vinyl ketone, stabilized	131P	1251
Molten sulfur	133	2448
Molten sulphur	133	2448
Molybdenum pentachloride	156	2508
Monoethanolamine	153	2491
Mononitrotoluidines	153	2660
Morpholine	132	2054
Motor fuel anti-knock mixture	152	1649
Motor fuel anti-knock mixture, flammable	131	3483
Motor spirit	128	1203
Motor spirit and ethanol mixture, with more than 10% ethanol	127	3475
Muriatic acid	157	1789
Musk xylene	149	2956
Mustard	153	——
Mustard Lewisite	153	——
Naphthalene, crude	133	1334
Naphthalene, molten	133	2304
Naphthalene, refined	133	1334
Naphthylamine (alpha)	153	2077
Naphthylamine (beta), solid	153	1650
Naphthylamine (beta), solution	153	3411
Naphthylthiourea	153	1651
Naphthylurea	153	1652
Natural gas, compressed	115	1971
Natural gas, refrigerated liquid (cryogenic liquid)	115	1972
Neohexane	128	1208
Neon	120	1065
Neon, compressed	120	1065
Neon, refrigerated liquid (cryogenic liquid)	120	1913
Nickel carbonyl	131	1259
Nickel catalyst, dry	135	2881
Nickel cyanide	151	1653
Nickel nitrate	140	2725
Nickel nitrite	140	2726
Nicotine	151	1654
Nicotine compound, liquid, n.o.s.	151	3144
Nicotine compound, solid, n.o.s.	151	1655
Nicotine hydrochloride, liquid	151	1656
Nicotine hydrochloride, solid	151	3444
Nicotine hydrochloride, solution	151	1656
Nicotine preparation, liquid, n.o.s.	151	3144
Nicotine preparation, solid, n.o.s.	151	1655
Nicotine salicylate	151	1657
Nicotine sulfate, solid	151	3445
Nicotine sulfate, solution	151	1658
Nicotine sulphate, solid	151	3445
Nicotine sulphate, solution	151	1658
Nicotine tartrate	151	1659
Nitrates, inorganic, aqueous solution, n.o.s.	140	3218
Nitrates, inorganic, n.o.s.	140	1477

Name of Material	Guide No.	ID No.
Nitrating acid mixture with more than 50% nitric acid	157	1796
Nitrating acid mixture with not more than 50% nitric acid	157	1796
Nitrating acid mixture, spent, with more than 50% nitric acid	157	1826
Nitrating acid mixture, spent, with not more than 50% nitric acid	157	1826
Nitric acid, other than red fuming, with more than 65% nitric acid	157	2031
Nitric acid, other than red fuming, with not more than 65% nitric acid	157	2031
Nitric acid, red fuming	157	2032
Nitric oxide	124	1660
Nitric oxide, compressed	124	1660
Nitric oxide and Dinitrogen tetroxide mixture	124	1975
Nitric oxide and Nitrogen dioxide mixture	124	1975
Nitriles, flammable, poisonous, n.o.s.	131	3273
Nitriles, flammable, toxic, n.o.s.	131	3273
Nitriles, liquid, poisonous, n.o.s.	151	3276
Nitriles, liquid, toxic, n.o.s.	151	3276
Nitriles, poisonous, flammable, n.o.s.	131	3275
Nitriles, poisonous, liquid, n.o.s.	151	3276
Nitriles, poisonous, solid, n.o.s.	151	3439
Nitriles, solid, poisonous, n.o.s.	151	3439
Nitriles, solid, toxic, n.o.s.	151	3439
Nitriles, toxic, flammable, n.o.s.	131	3275
Nitriles, toxic, liquid, n.o.s.	151	3276
Nitriles, toxic, solid, n.o.s.	151	3439
Nitrites, inorganic, aqueous solution, n.o.s.	140	3219
Nitrites, inorganic, n.o.s.	140	2627
Nitroanilines	153	1661
Nitroanisoles, liquid	152	2730
Nitroanisoles, solid	152	3458
Nitrobenzene	152	1662
Nitrobenzenesulfonic acid	153	2305
Nitrobenzenesulphonic acid	153	2305
Nitrobenzotrifluorides, liquid	152	2306
Nitrobenzotrifluorides, solid	152	3431
Nitrobromobenzenes, liquid	152	2732
Nitrobromobenzenes, solid	152	3459
Nitrocellulose membrane filters	133	3270
Nitrocellulose mixture, without pigment	133	2557
Nitrocellulose mixture, without plasticizer	133	2557
Nitrocellulose mixture, with pigment	133	2557
Nitrocellulose mixture, with plasticizer	133	2557
Nitrocellulose, solution, flammable	127	2059
Nitrocellulose with alcohol, not less than 25% alcohol	113	2556
Nitrocellulose with water, not less than 25% water	113	2555
3-Nitro-4-chlorobenzotrifluoride	152	2307
Nitrocresols, liquid	153	3434
Nitrocresols, solid	153	2446

Name of Material	Guide No.	ID No.
Nitroethane	129	2842
Nitrogen	120	1066
Nitrogen, compressed	120	1066
Nitrogen, refrigerated liquid (cryogenic liquid)	120	1977
Nitrogen dioxide	124	1067
Nitrogen dioxide and Nitric oxide mixture	124	1975
Nitrogen trifluoride	122	2451
Nitrogen trifluoride, compressed	122	2451
Nitrogen trioxide	124	2421
Nitroglycerin, solution in alcohol, with more than 1% but not more than 5% Nitroglycerin	127	3064
Nitroglycerin, solution in alcohol, with not more than 1% Nitroglycerin	127	1204
Nitroglycerin mixture, desensitized, liquid, flammable, n.o.s., with not more than 30% Nitroglycerin	113	3343
Nitroglycerin mixture, desensitized, liquid, n.o.s., with not more than 30% Nitroglycerin	113	3357
Nitroglycerin mixture, desensitized, solid, n.o.s., with more than 2% but not more than 10% Nitroglycerin	113	3319
Nitroguanidine, wetted with not less than 20% water	113	1336
Nitrohydrochloric acid	157	1798
Nitromethane	129	1261
Nitronaphthalene	133	2538
Nitrophenols	153	1663
4-Nitrophenylhydrazine, with not less than 30% water	113	3376
Nitropropanes	129	2608
p-Nitrosodimethylaniline	135	1369
Nitrostarch, wetted with not less than 20% water	113	1337
Nitrosyl chloride	125	1069
Nitrosylsulfuric acid, liquid	157	2308
Nitrosylsulfuric acid, solid	157	3456
Nitrosylsulphuric acid, liquid	157	2308
Nitrosylsulphuric acid, solid	157	3456
Nitrotoluenes, liquid	152	1664
Nitrotoluenes, solid	152	3446
Nitrotoluidines (mono)	153	2660
Nitrous oxide	122	1070
Nitrous oxide, compressed	122	1070
Nitrous oxide, refrigerated liquid	122	2201
Nitrous oxide and Carbon dioxide mixture	126	1015
Nitroxylenes, liquid	152	1665
Nitroxylenes, solid	152	3447
Nonanes	128	1920
Nonyltrichlorosilane	156	1799
2,5-Norbornadiene, stabilized	128P	2251
Octadecyltrichlorosilane	156	1800
Octadiene	128P	2309
Octafluorobut-2-ene	126	2422
Octafluorocyclobutane	126	1976
Octafluoropropane	126	2424
Octanes	128	1262
Octyl aldehydes	129	1191
Octyltrichlorosilane	156	1801
Oil, petroleum	128	1270
Oil gas	119	1071

Name of Material	Guide No.	ID No.
Oil gas, compressed	119	1071
Organic peroxide type B, liquid	146	3101
Organic peroxide type B, liquid, temperature controlled	148	3111
Organic peroxide type B, solid	146	3102
Organic peroxide type B, solid, temperature controlled	148	3112
Organic peroxide type C, liquid	146	3103
Organic peroxide type C, liquid, temperature controlled	148	3113
Organic peroxide type C, solid	146	3104
Organic peroxide type C, solid, temperature controlled	148	3114
Organic peroxide type D, liquid	145	3105
Organic peroxide type D, liquid, temperature controlled	148	3115
Organic peroxide type D, solid	145	3106
Organic peroxide type D, solid, temperature controlled	148	3116
Organic peroxide type E, liquid	145	3107
Organic peroxide type E, liquid, temperature controlled	148	3117
Organic peroxide type E, solid	145	3108
Organic peroxide type E, solid, temperature controlled	148	3118
Organic peroxide type F, liquid	145	3109
Organic peroxide type F, liquid, temperature controlled	148	3119
Organic peroxide type F, solid	145	3110
Organic peroxide type F, solid, temperature controlled	148	3120
Organic phosphate compound mixed with compressed gas	123	1955
Organic phosphate mixed with compressed gas	123	1955
Organic phosphorus compound mixed with compressed gas	123	1955
Organic pigments, self-heating	135	3313
Organoarsenic compound, liquid, n.o.s.	151	3280
Organoarsenic compound, solid, n.o.s.	151	3465
Organochlorine pesticide, liquid, flammable, poisonous	131	2762
Organochlorine pesticide, liquid, flammable, toxic	131	2762
Organochlorine pesticide, liquid, poisonous	151	2996
Organochlorine pesticide, liquid, poisonous, flammable	131	2995
Organochlorine pesticide, liquid, toxic	151	2996
Organochlorine pesticide, liquid, toxic, flammable	131	2995
Organochlorine pesticide, solid, poisonous	151	2761
Organochlorine pesticide, solid, toxic	151	2761
Organometallic compound, liquid, poisonous, n.o.s.	151	3282
Organometallic compound, liquid, toxic, n.o.s.	151	3282
Organometallic compound, poisonous, liquid, n.o.s.	151	3282
Organometallic compound, poisonous, solid, n.o.s.	151	3467
Organometallic compound, solid, poisonous, n.o.s.	151	3467
Organometallic compound, solid, toxic, n.o.s.	151	3467
Organometallic compound, toxic, liquid, n.o.s.	151	3282

Name of Material	Guide No.	ID No.
Organometallic compound, toxic, solid, n.o.s.	151	3467
Organometallic substance, liquid, pyrophoric	135	3392
Organometallic substance, liquid, pyrophoric, water-reactive	135	3394
Organometallic substance, liquid, water-reactive	135	3398
Organometallic substance, liquid, water-reactive, flammable	138	3399
Organometallic substance, solid, pyrophoric	135	3391
Organometallic substance, solid, pyrophoric, water-reactive	135	3393
Organometallic substance, solid, self-heating	138	3400
Organometallic substance, solid, water-reactive	135	3395
Organometallic substance, solid, water-reactive, flammable	138	3396
Organometallic substance, solid, water-reactive, self-heating	138	3397
Organophosphorus compound, liquid, poisonous, n.o.s.	151	3278
Organophosphorus compound, liquid, toxic, n.o.s.	151	3278
Organophosphorus compound, poisonous, flammable, n.o.s.	131	3279
Organophosphorus compound, poisonous, liquid, n.o.s.	151	3278
Organophosphorus compound, poisonous, solid, n.o.s.	151	3464
Organophosphorus compound, solid, poisonous, n.o.s.	151	3464
Organophosphorus compound, solid, toxic, n.o.s.	151	3464
Organophosphorus compound, toxic, flammable, n.o.s.	131	3279
Organophosphorus compound, toxic, liquid, n.o.s.	151	3278
Organophosphorus compound, toxic, solid, n.o.s.	151	3464
Organophosphorus pesticide, liquid, flammable, poisonous	131	2784
Organophosphorus pesticide, liquid, flammable, toxic	131	2784
Organophosphorus pesticide, liquid, poisonous	152	3018
Organophosphorus pesticide, liquid, poisonous, flammable	131	3017
Organophosphorus pesticide, liquid, toxic	152	3018
Organophosphorus pesticide, liquid, toxic, flammable	131	3017
Organophosphorus pesticide, solid, poisonous	152	2783
Organophosphorus pesticide, solid, toxic	152	2783
Organotin compound, liquid, n.o.s.	153	2788
Organotin compound, solid, n.o.s.	153	3146
Organotin pesticide, liquid, flammable, poisonous	131	2787
Organotin pesticide, liquid, flammable, toxic	131	2787
Organotin pesticide, liquid, poisonous	153	3020
Organotin pesticide, liquid, poisonous, flammable	131	3019
Organotin pesticide, liquid, toxic	153	3020
Organotin pesticide, liquid, toxic, flammable	131	3019
Organotin pesticide, solid, poisonous	153	2786

Name of Material	Guide No.	ID No.
Organotin pesticide, solid, toxic	153	2786
Osmium tetroxide	154	2471
Other regulated substances, liquid, n.o.s.	171	3082
Other regulated substances, solid, n.o.s.	171	3077
Oxidizing liquid, corrosive, n.o.s.	140	3098
Oxidizing liquid, n.o.s.	140	3139
Oxidizing liquid, poisonous, n.o.s.	142	3099
Oxidizing liquid, toxic, n.o.s.	142	3099
Oxidizing solid, corrosive, n.o.s.	140	3085
Oxidizing solid, flammable, n.o.s.	140	3137
Oxidizing solid, n.o.s.	140	1479
Oxidizing solid, poisonous, n.o.s.	141	3087
Oxidizing solid, self-heating, n.o.s.	135	3100
Oxidizing solid, toxic, n.o.s.	141	3087
Oxidizing solid, water-reactive, n.o.s.	144	3121
Oxygen	122	1072
Oxygen, compressed	122	1072
Oxygen, refrigerated liquid (cryogenic liquid)	122	1073
Oxygen and Carbon dioxide mixture, compressed	122	1014
Oxygen difluoride	124	2190
Oxygen difluoride, compressed	124	2190
Oxygen generator, chemical	140	3356
Oxygen generator, chemical, spent	140	3356
Packagings discarded, empty, uncleaned	171	3509
Paint (corrosive)	153	3066
Paint, corrosive, flammable	132	3470
Paint (flammable)	128	1263
Paint, flammable, corrosive	132	3469
Paint related material (corrosive)	153	3066
Paint related material, corrosive, flammable	132	3470
Paint related material (flammable)	128	1263
Paint related material, flammable, corrosive	132	3469
Paper, unsaturated oil treated	133	1379
Paraformaldehyde	133	2213
Paraldehyde	129	1264
Parathion and compressed gas mixture	123	1967
PCB	171	2315
PD	152	——
Pentaborane	135	1380
Pentachloroethane	151	1669
Pentachlorophenol	154	3155
Pentaerythrite tetranitrate mixture, desensitized, solid, n.o.s., with more than 10% but not more than 20% PETN	113	3344
Pentaerythritol tetranitrate mixture, desensitized, solid, n.o.s., with more than 10% but not more than 20% PETN	113	3344
Pentafluoroethane	126	3220
Pentafluoroethane and Ethylene oxide mixture, with not more than 7.9% Ethylene oxide	126	3298
Pentamethylheptane	128	2286

Name of Material	Guide No.	ID No.
Pentane-2,4-dione	131	2310
Pentanes	128	1265
Pentanols	129	1105
1-Pentene	128	1108
1-Pentol	153P	2705
Perchlorates, inorganic, aqueous solution, n.o.s.	140	3211
Perchlorates, inorganic, n.o.s.	140	1481
Perchloric acid, with more than 50% but not more than 72% acid	143	1873
Perchloric acid, with not more than 50% acid	157	1802
Perchloroethylene	160	1897
Perchloromethyl mercaptan	157	1670
Perchloryl fluoride	124	3083
Perfluoro(ethyl vinyl ether)	115	3154
Perfluoro(methyl vinyl ether)	115	3153
Perfumery products, with flammable solvents	127	1266
Permanganates, inorganic, aqueous solution, n.o.s.	140	3214
Permanganates, inorganic, n.o.s.	140	1482
Peroxides, inorganic, n.o.s.	140	1483
Peroxyacetic acid and hydrogen peroxide mixture, with acid(s), water and not more than 5% Peroxyacetic acid, stabilized	140	3149
Persulfates, inorganic, aqueous solution, n.o.s.	140	3216
Persulfates, inorganic, n.o.s.	140	3215
Persulphates, inorganic, aqueous solution, n.o.s.	140	3216
Persulphates, inorganic, n.o.s.	140	3215
Pesticide, liquid, flammable, poisonous, n.o.s.	131	3021
Pesticide, liquid, flammable, toxic, n.o.s.	131	3021
Pesticide, liquid, poisonous, flammable, n.o.s.	131	2903
Pesticide, liquid, poisonous, n.o.s.	151	2902
Pesticide, liquid, toxic, flammable, n.o.s.	131	2903
Pesticide, liquid, toxic, n.o.s.	151	2902
Pesticide, solid, poisonous, n.o.s.	151	2588
Pesticide, solid, toxic, n.o.s.	151	2588
PETN mixture, desensitized, solid, n.o.s., with more than 10% but not more than 20% PETN	113	3344
Petrol	128	1203
Petrol and ethanol mixture, with more than 10% ethanol	127	3475
Petroleum crude oil	128	1267
Petroleum distillates, n.o.s.	128	1268
Petroleum gases, liquefied	115	1075
Petroleum oil	128	1270
Petroleum products, n.o.s.	128	1268
Petroleum sour crude oil, flammable, poisonous	131	3494
Petroleum sour crude oil, flammable, toxic	131	3494
Phenacyl bromide	153	2645
Phenetidines	153	2311
Phenol, molten	153	2312
Phenol, solid	153	1671
Phenol solution	153	2821
Phenolates, liquid	154	2904
Phenolates, solid	154	2905

Name of Material	Guide No.	ID No.
Phenolsulfonic acid, liquid	153	1803
Phenolsulphonic acid, liquid	153	1803
Phenoxyacetic acid derivative pesticide, liquid, flammable, poisonous	131	3346
Phenoxyacetic acid derivative pesticide, liquid, flammable, toxic	131	3346
Phenoxyacetic acid derivative pesticide, liquid, poisonous	153	3348
Phenoxyacetic acid derivative pesticide, liquid, poisonous, flammable	131	3347
Phenoxyacetic acid derivative pesticide, liquid, toxic	153	3348
Phenoxyacetic acid derivative pesticide, liquid, toxic, flammable	131	3347
Phenoxyacetic acid derivative pesticide, solid, poisonous	153	3345
Phenoxyacetic acid derivative pesticide, solid, toxic	153	3345
Phenylacetonitrile, liquid	152	2470
Phenylacetyl chloride	156	2577
Phenylcarbylamine chloride	151	1672
Phenyl chloroformate	156	2746
Phenylenediamines	153	1673
Phenylhydrazine	153	2572
Phenyl isocyanate	155	2487
Phenyl mercaptan	131	2337
Phenylmercuric acetate	151	1674
Phenylmercuric compound, n.o.s.	151	2026
Phenylmercuric hydroxide	151	1894
Phenylmercuric nitrate	151	1895
Phenylphosphorus dichloride	137	2798
Phenylphosphorus thiodichloride	137	2799
Phenyltrichlorosilane	156	1804
Phenyl urea pesticide, liquid, poisonous	151	3002
Phenyl urea pesticide, liquid, toxic	151	3002
Phosgene	125	1076
9-Phosphabicyclononanes	135	2940
Phosphine	119	2199
Phosphine, adsorbed	173	3525
Phosphoric acid, solid	154	3453
Phosphoric acid, solution	154	1805
Phosphorous acid	154	2834
Phosphorus, amorphous	133	1338
Phosphorus, white, dry or under water or in solution	136	1381
Phosphorus, white, molten	136	2447
Phosphorus, yellow, dry or under water or in solution	136	1381
Phosphorus heptasulfide, free from yellow and white Phosphorus	139	1339
Phosphorus heptasulphide, free from yellow and white Phosphorus	139	1339
Phosphorus oxybromide, molten	137	2576
Phosphorus oxybromide, solid	137	1939
Phosphorus oxychloride	137	1810
Phosphorus pentabromide	137	2691
Phosphorus pentachloride	137	1806
Phosphorus pentafluoride	125	2198
Phosphorus pentafluoride, adsorbed	173	3524
Phosphorus pentafluoride, compressed	125	2198

Name of Material	Guide No.	ID No.
Phosphorus pentasulfide, free from yellow and white Phosphorus	139	1340
Phosphorus pentasulphide, free from yellow and white Phosphorus	139	1340
Phosphorus pentoxide	137	1807
Phosphorus sesquisulfide, free from yellow and white Phosphorus	139	1341
Phosphorus sesquisulphide, free from yellow and white Phosphorus	139	1341
Phosphorus tribromide	137	1808
Phosphorus trichloride	137	1809
Phosphorus trioxide	157	2578
Phosphorus trisulfide, free from yellow and white Phosphorus	139	1343
Phosphorus trisulphide, free from yellow and white Phosphorus	139	1343
Phthalic anhydride	156	2214
Picolines	129	2313
Picric acid, wetted with not less than 10% water	113	3364
Picric acid, wetted with not less than 30% water	113	1344
Picrite, wetted with not less than 20% water	113	1336
Picryl chloride, wetted with not less than 10% water	113	3365
Pinene (alpha)	128	2368
Pine oil	129	1272
Piperazine	153	2579
Piperidine	132	2401
Plastic molding compound	171	3314
Plastics moulding compound	171	3314
Plastics, nitrocellulose-based, self-heating, n.o.s.	135	2006
Poisonous by inhalation liquid, corrosive, flammable, n.o.s. (Inhalation Hazard Zone A)	131	3492
Poisonous by inhalation liquid, corrosive, flammable, n.o.s. (Inhalation Hazard Zone B)	131	3493
Poisonous by inhalation liquid, corrosive, n.o.s. (Inhalation Hazard Zone A)	154	3389
Poisonous by inhalation liquid, corrosive, n.o.s. (Inhalation Hazard Zone B)	154	3390
Poisonous by inhalation liquid, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)	131	3488
Poisonous by inhalation liquid, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)	131	3489
Poisonous by inhalation liquid, flammable, n.o.s. (Inhalation Hazard Zone A)	131	3383
Poisonous by inhalation liquid, flammable, n.o.s. (Inhalation Hazard Zone B)	131	3384
Poisonous by inhalation liquid, n.o.s. (Inhalation Hazard Zone A)	151	3381
Poisonous by inhalation liquid, n.o.s. (Inhalation Hazard Zone B)	151	3382
Poisonous by inhalation liquid, oxidizing, n.o.s. (Inhalation Hazard Zone A)	142	3387
Poisonous by inhalation liquid, oxidizing, n.o.s. (Inhalation Hazard Zone B)	142	3388
Poisonous by inhalation liquid, water-reactive, flammable, n.o.s. (Inhalation Hazard Zone A)	155	3490

Name of Material	Guide No.	ID No.
Poisonous by inhalation liquid, water-reactive, flammable, n.o.s. (Inhalation Hazard Zone B)	**155**	3491
Poisonous by inhalation liquid, water-reactive, n.o.s. (Inhalation Hazard Zone A)	**139**	3385
Poisonous by inhalation liquid, water-reactive, n.o.s. (Inhalation Hazard Zone B)	**139**	3386
Poisonous liquid, corrosive, inorganic, n.o.s.	**154**	3289
Poisonous liquid, corrosive, organic, n.o.s.	**154**	2927
Poisonous liquid, flammable, organic, n.o.s.	**131**	2929
Poisonous liquid, inorganic, n.o.s.	**151**	3287
Poisonous liquid, organic, n.o.s.	**153**	2810
Poisonous liquid, oxidizing, n.o.s.	**142**	3122
Poisonous liquid, water-reactive, n.o.s.	**139**	3123
Poisonous solid, corrosive, inorganic, n.o.s.	**154**	3290
Poisonous solid, corrosive, organic, n.o.s.	**154**	2928
Poisonous solid, flammable, organic, n.o.s.	**134**	2930
Poisonous solid, inorganic, n.o.s.	**151**	3288
Poisonous solid, organic, n.o.s.	**154**	2811
Poisonous solid, oxidizing, n.o.s.	**141**	3086
Poisonous solid, self-heating, n.o.s.	**136**	3124
Poisonous solid, water-reactive, n.o.s.	**139**	3125
Polyamines, flammable, corrosive, n.o.s.	**132**	2733
Polyamines, liquid, corrosive, flammable, n.o.s.	**132**	2734
Polyamines, liquid, corrosive, n.o.s.	**153**	2735
Polyamines, solid, corrosive, n.o.s.	**154**	3259
Polychlorinated biphenyls, liquid	**171**	2315
Polychlorinated biphenyls, solid	**171**	3432
Polyester resin kit, liquid base material	**128**	3269
Polyester resin kit, solid base material	**128P**	3527
Polyhalogenated biphenyls, liquid	**171**	3151
Polyhalogenated biphenyls, solid	**171**	3152
Polyhalogenated terphenyls, liquid	**171**	3151
Polyhalogenated terphenyls, solid	**171**	3152
Polymeric beads, expandable	**171**	2211
Polymerizing substance, liquid, stabilized, n.o.s.	**149P**	3532
Polymerizing substance, liquid, temperature controlled, n.o.s.	**150P**	3534
Polymerizing substance, solid, stabilized, n.o.s.	**149P**	3531
Polymerizing substance, solid, temperature controlled, n.o.s.	**150P**	3533
Potassium	**138**	2257
Potassium, metal alloys, liquid	**138**	1420
Potassium, metal alloys, solid	**138**	3403
Potassium arsenate	**151**	1677
Potassium arsenite	**154**	1678
Potassium borohydride	**138**	1870

Name of Material	Guide No.	ID No.
Potassium bromate	140	1484
Potassium chlorate	140	1485
Potassium chlorate, aqueous solution	140	2427
Potassium cuprocyanide	157	1679
Potassium cyanide, solid	157	1680
Potassium cyanide, solution	157	3413
Potassium dithionite	135	1929
Potassium fluoride, solid	154	1812
Potassium fluoride, solution	154	3422
Potassium fluoroacetate	151	2628
Potassium fluorosilicate	151	2655
Potassium hydrogen difluoride, solid	154	1811
Potassium hydrogen difluoride, solution	154	3421
Potassium hydrogen sulfate	154	2509
Potassium hydrogen sulphate	154	2509
Potassium hydrosulfite	135	1929
Potassium hydrosulphite	135	1929
Potassium hydroxide, solid	154	1813
Potassium hydroxide, solution	154	1814
Potassium metavanadate	151	2864
Potassium monoxide	154	2033
Potassium nitrate	140	1486
Potassium nitrate and Sodium nitrate mixture	140	1499
Potassium nitrate and Sodium nitrite mixture	140	1487
Potassium nitrite	140	1488
Potassium perchlorate	140	1489
Potassium permanganate	140	1490
Potassium peroxide	144	1491
Potassium persulfate	140	1492
Potassium persulphate	140	1492
Potassium phosphide	139	2012
Potassium sodium alloys, liquid	138	1422
Potassium sodium alloys, solid	138	3404
Potassium sulfide, anhydrous	135	1382
Potassium sulfide, hydrated, with not less than 30% water of crystallization	153	1847
Potassium sulfide, with less than 30% water of crystallization	135	1382
Potassium sulphide, anhydrous	135	1382
Potassium sulphide, hydrated, with not less than 30% water of crystallization	153	1847
Potassium sulphide, with less than 30% water of crystallization	135	1382
Potassium superoxide	143	2466
Printing ink, flammable	129	1210
Printing ink related material, flammable	129	1210
Propadiene, stabilized	116P	2200
Propadiene and Methylacetylene mixture, stabilized	116P	1060
Propane	115	1075
Propane	115	1978
Propane-Ethane mixture, refrigerated liquid	115	1961
Propanethiols	130	2402
n-Propanol	129	1274
Propionaldehyde	129P	1275
Propionic acid	153	1848
Propionic acid, with not less than 10% and less than 90% acid	153	1848

Name of Material	Guide No.	ID No.
Propionic acid, with not less than 90% acid	153	3463
Propionic anhydride	156	2496
Propionitrile	131	2404
Propionyl chloride	132	1815
n-Propyl acetate	129	1276
Propyl alcohol, normal	129	1274
Propylamine	132	1277
n-Propyl benzene	128	2364
Propyl chloride	129	1278
n-Propyl chloroformate	155	2740
Propylene	115	1075
Propylene	115	1077
Propylene, Ethylene and Acetylene in mixture, refrigerated liquid containing at least 71.5% Ethylene with not more than 22.5% Acetylene and not more than 6% Propylene	115	3138
Propylene chlorohydrin	131	2611
1,2-Propylenediamine	132	2258
Propyleneimine, stabilized	131P	1921
Propylene oxide	127P	1280
Propylene oxide and Ethylene oxide mixture, with not more than 30% Ethylene oxide	131P	2983
Propylene tetramer	128	2850
Propyl formates	129	1281
n-Propyl isocyanate	155P	2482
n-Propyl nitrate	128	1865
Propyltrichlorosilane	155	1816
Pyrethroid pesticide, liquid, flammable, poisonous	131	3350
Pyrethroid pesticide, liquid, flammable, toxic	131	3350
Pyrethroid pesticide, liquid, poisonous	151	3352
Pyrethroid pesticide, liquid, poisonous, flammable	131	3351
Pyrethroid pesticide, liquid, toxic	151	3352
Pyrethroid pesticide, liquid, toxic, flammable	131	3351
Pyrethroid pesticide, solid, poisonous	151	3349
Pyrethroid pesticide, solid, toxic	151	3349
Pyridine	129	1282
Pyrophoric alloy, n.o.s.	135	1383
Pyrophoric liquid, inorganic, n.o.s.	135	3194
Pyrophoric liquid, organic, n.o.s.	135	2845
Pyrophoric metal, n.o.s.	135	1383
Pyrophoric solid, inorganic, n.o.s.	135	3200
Pyrophoric solid, organic, n.o.s.	135	2846
Pyrosulfuryl chloride	137	1817
Pyrosulphuryl chloride	137	1817
Pyrrolidine	132	1922
Quinoline	154	2656
Radioactive material, excepted package, articles	161	2911
Radioactive material, excepted package, articles manufactured from depleted Uranium	161	2909
Radioactive material, excepted package, articles manufactured from natural Thorium	161	2909

Name of Material	Guide No.	ID No.
Radioactive material, excepted package, articles manufactured from natural Uranium	**161**	2909
Radioactive material, excepted package, empty packaging	**161**	2908
Radioactive material, excepted package, instruments	**161**	2911
Radioactive material, excepted package, limited quantity of material	**161**	2910
Radioactive material, low specific activity (LSA-I), non fissile or fissile-excepted	**162**	2912
Radioactive material, low specific activity (LSA-II), fissile	**165**	3324
Radioactive material, low specific activity (LSA-II), non fissile or fissile-excepted	**162**	3321
Radioactive material, low specific activity (LSA-III), fissile	**165**	3325
Radioactive material, low specific activity (LSA-III), non fissile or fissile-excepted	**162**	3322
Radioactive material, surface contaminated objects (SCO-I), fissile	**165**	3326
Radioactive material, surface contaminated objects (SCO-I), non fissile or fissile-excepted	**162**	2913
Radioactive material, surface contaminated objects (SCO-II), fissile	**165**	3326
Radioactive material, surface contaminated objects (SCO-II), non fissile or fissile-excepted	**162**	2913
Radioactive material, transported under special arrangement, fissile	**165**	3331
Radioactive material, transported under special arrangement, non fissile or fissile-excepted	**163**	2919
Radioactive material, Type A package, fissile, non-special form	**165**	3327
Radioactive material, Type A package, non-special form, non fissile or fissile-excepted	**163**	2915
Radioactive material, Type A package, special form, fissile	**165**	3333
Radioactive material, Type A package, special form, non fissile or fissile-excepted	**164**	3332
Radioactive material, Type B(M) package, fissile	**165**	3329
Radioactive material, Type B(M) package, non fissile or fissile-excepted	**163**	2917
Radioactive material, Type B(U) package, fissile	**165**	3328
Radioactive material, Type B(U) package, non fissile or fissile-excepted	**163**	2916
Radioactive material, Type C package, fissile	**165**	3330
Radioactive material, Type C package, non fissile or fissile excepted	**163**	3323
Radioactive material, Uranium hexafluoride, fissile	**166**	2977
Radioactive material, Uranium hexafluoride, non fissile or fissile-excepted	**166**	2978
Rags, oily	**133**	1856

Name of Material	Guide No.	ID No.
Receptacles, small, containing gas	115	2037
Red phosphorus	133	1338
Refrigerant gas, n.o.s.	126	1078
Refrigerant gases, n.o.s. (flammable)	115	1954
Refrigerant gas R-12	126	1028
Refrigerant gas R-12B1	126	1974
Refrigerant gas R-12B2	171	1941
Refrigerant gas R-13	126	1022
Refrigerant gas R-13B1	126	1009
Refrigerant gas R-14	126	1982
Refrigerant gas R-14, compressed	126	1982
Refrigerant gas R-21	126	1029
Refrigerant gas R-22	126	1018
Refrigerant gas R-23	126	1984
Refrigerant gas R-32	115	3252
Refrigerant gas R-40	115	1063
Refrigerant gas R-41	115	2454
Refrigerant gas R-114	126	1958
Refrigerant gas R-115	126	1020
Refrigerant gas R-116	126	2193
Refrigerant gas R-116, compressed	126	2193
Refrigerant gas R-124	126	1021
Refrigerant gas R-125	126	3220
Refrigerant gas R-133a	126	1983
Refrigerant gas R-134a	126	3159
Refrigerant gas R-142b	115	2517
Refrigerant gas R-143a	115	2035
Refrigerant gas R-152a	115	1030
Refrigerant gas R-161	115	2453
Refrigerant gas R-218	126	2424
Refrigerant gas R-227	126	3296
Refrigerant gas R-404A	126	3337
Refrigerant gas R-407A	126	3338
Refrigerant gas R-407B	126	3339
Refrigerant gas R-407C	126	3340
Refrigerant gas R-500	126	2602
Refrigerant gas R-502	126	1973
Refrigerant gas R-503	126	2599
Refrigerant gas R-1113	119P	1082
Refrigerant gas R-1132a	116P	1959
Refrigerant gas R-1216	126	1858
Refrigerant gas R-1318	126	2422
Refrigerant gas RC-318	126	1976
Refrigerating machines, containing Ammonia solutions (UN2672)	126	2857
Refrigerating machines, containing flammable, non-poisonous, liquefied gas	115	3358
Refrigerating machines, containing flammable, non-toxic, liquefied gas	115	3358
Refrigerating machines, containing non-flammable, non-poisonous gases	126	2857
Refrigerating machines, containing non-flammable, non-toxic gases	126	2857
Regulated medical waste, n.o.s.	158	3291
Resin solution	127	1866
Resorcinol	153	2876
Rosin oil	127	1286
Rubber scrap, powdered or granulated	133	1345

Name of Material	Guide No.	ID No.
Rubber shoddy, powdered or granulated	133	1345
Rubber solution	127	1287
Rubidium	138	1423
Rubidium hydroxide, solid	154	2678
Rubidium hydroxide, solution	154	2677
SA	119	——
Safety devices	171	3268
Sarin	153	——
Seat-belt pre-tensioners	171	3268
Seed cake, with more than 1.5% oil and not more than 11% moisture	135	1386
Seed cake, with not more than 1.5% oil and not more than 11% moisture	135	2217
Selenates	151	2630
Selenic acid	154	1905
Selenites	151	2630
Selenium compound, liquid, n.o.s.	151	3440
Selenium compound, solid, n.o.s.	151	3283
Selenium disulfide	153	2657
Selenium disulphide	153	2657
Selenium hexafluoride	125	2194
Selenium oxychloride	157	2879
Self-defense spray, non-pressurized	171	3334
Self-heating liquid, corrosive, inorganic, n.o.s.	136	3188
Self-heating liquid, corrosive, organic, n.o.s.	136	3185
Self-heating liquid, inorganic, n.o.s.	135	3186
Self-heating liquid, organic, n.o.s.	135	3183
Self-heating liquid, poisonous, inorganic, n.o.s.	136	3187
Self-heating liquid, poisonous, organic, n.o.s.	136	3184
Self-heating liquid, toxic, inorganic, n.o.s.	136	3187
Self-heating liquid, toxic, organic, n.o.s.	136	3184
Self-heating solid, corrosive, inorganic, n.o.s.	136	3192
Self-heating solid, corrosive, organic, n.o.s.	136	3126
Self-heating solid, inorganic, n.o.s.	135	3190
Self-heating solid, organic, n.o.s.	135	3088
Self-heating solid, oxidizing, n.o.s.	135	3127
Self-heating solid, poisonous, inorganic, n.o.s.	136	3191
Self-heating solid, poisonous, organic, n.o.s.	136	3128
Self-heating solid, toxic, inorganic, n.o.s.	136	3191
Self-heating solid, toxic, organic, n.o.s.	136	3128
Self-reactive liquid type B	149	3221
Self-reactive liquid type B, temperature controlled	150	3231
Self-reactive liquid type C	149	3223
Self-reactive liquid type C, temperature controlled	150	3233
Self-reactive liquid type D	149	3225
Self-reactive liquid type D, temperature controlled	150	3235
Self-reactive liquid type E	149	3227
Self-reactive liquid type E, temperature controlled	150	3237
Self-reactive liquid type F	149	3229

Name of Material	Guide No.	ID No.
Self-reactive liquid type F, temperature controlled	150	3239
Self-reactive solid type B	149	3222
Self-reactive solid type B, temperature controlled	150	3232
Self-reactive solid type C	149	3224
Self-reactive solid type C, temperature controlled	150	3234
Self-reactive solid type D	149	3226
Self-reactive solid type D, temperature controlled	150	3236
Self-reactive solid type E	149	3228
Self-reactive solid type E, temperature controlled	150	3238
Self-reactive solid type F	149	3230
Self-reactive solid type F, temperature controlled	150	3240
Shale oil	128	1288
Silane	116	2203
Silane, compressed	116	2203
Silicon powder, amorphous	170	1346
Silicon tetrachloride	157	1818
Silicon tetrafluoride	125	1859
Silicon tetrafluoride, adsorbed	173	3521
Silicon tetrafluoride, compressed	125	1859
Silver arsenite	151	1683
Silver cyanide	151	1684
Silver nitrate	140	1493
Silver picrate, wetted with not less than 30% water	113	1347
Sludge acid	153	1906
Smokeless powder for small arms	133	3178
Soda lime, with more than 4% Sodium hydroxide	154	1907
Sodium	138	1428
Sodium aluminate, solid	154	2812
Sodium aluminate, solution	154	1819
Sodium aluminum hydride	138	2835
Sodium ammonium vanadate	154	2863
Sodium arsanilate	154	2473
Sodium arsenate	151	1685
Sodium arsenite, aqueous solution	154	1686
Sodium arsenite, solid	151	2027
Sodium azide	153	1687
Sodium, batteries containing	138	3292
Sodium bisulfate, solution	154	2837
Sodium bisulphate, solution	154	2837
Sodium borohydride	138	1426
Sodium borohydride and Sodium hydroxide solution, with not more than 12% Sodium borohydride and not more than 40% Sodium hydroxide	157	3320
Sodium bromate	140	1494
Sodium cacodylate	152	1688
Sodium carbonate peroxyhydrate	140	3378
Sodium chlorate	140	1495
Sodium chlorate, aqueous solution	140	2428
Sodium chlorite	143	1496
Sodium chloroacetate	151	2659
Sodium cuprocyanide, solid	157	2316
Sodium cuprocyanide, solution	157	2317
Sodium cyanide, solid	157	1689
Sodium cyanide, solution	157	3414
Sodium dichloroisocyanurate	140	2465

Name of Material	Guide No.	ID No.
Sodium dichloro-s-triazinetrione	140	2465
Sodium dinitro-o-cresolate, wetted with not less than 10% water	113	3369
Sodium dinitro-o-cresolate, wetted with not less than 15% water	113	1348
Sodium dithionite	135	1384
Sodium fluoride, solid	154	1690
Sodium fluoride, solution	154	3415
Sodium fluoroacetate	151	2629
Sodium fluorosilicate	154	2674
Sodium hydride	138	1427
Sodium hydrogendifluoride	154	2439
Sodium hydrosulfide, hydrated, with not less than 25% water of crystallization	154	2949
Sodium hydrosulfide, with less than 25% water of crystallization	135	2318
Sodium hydrosulfide, with not less than 25% water of crystallization	154	2949
Sodium hydrosulfite	135	1384
Sodium hydrosulphide, hydrated, with not less than 25% water of crystallization	154	2949
Sodium hydrosulphide, with less than 25% water of crystallization	135	2318
Sodium hydrosulphide, with not less than 25% water of crystallization	154	2949
Sodium hydrosulphite	135	1384
Sodium hydroxide, solid	154	1823
Sodium hydroxide, solution	154	1824
Sodium hypochlorite	154	1791
Sodium methylate, dry	138	1431
Sodium methylate, solution in alcohol	132	1289
Sodium monoxide	157	1825
Sodium nitrate	140	1498
Sodium nitrate and Potassium nitrate mixture	140	1499
Sodium nitrite	141	1500
Sodium nitrite and Potassium nitrate mixture	140	1487
Sodium pentachlorophenate	154	2567
Sodium perborate monohydrate	140	3377
Sodium perchlorate	140	1502
Sodium permanganate	140	1503
Sodium peroxide	144	1504
Sodium peroxoborate, anhydrous	140	3247
Sodium persulfate	140	1505
Sodium persulphate	140	1505
Sodium phosphide	139	1432
Sodium picramate, wetted with not less than 20% water	113	1349
Sodium potassium alloys, liquid	138	1422
Sodium potassium alloys, solid	138	3404
Sodium sulfide, anhydrous	135	1385
Sodium sulfide, hydrated, with not less than 30% water	153	1849
Sodium sulfide, with less than 30% water of crystallization	135	1385
Sodium sulphide, anhydrous	135	1385
Sodium sulphide, hydrated, with not less than 30% water	153	1849
Sodium sulphide, with less than 30% water of crystallization	135	1385
Sodium superoxide	143	2547

Name of Material	Guide No.	ID No.
Solids containing corrosive liquid, n.o.s.	154	3244
Solids containing flammable liquid, n.o.s.	133	3175
Solids containing poisonous liquid, n.o.s.	151	3243
Solids containing toxic liquid, n.o.s.	151	3243
Soman	153	——
Stannic chloride, anhydrous	137	1827
Stannic chloride, pentahydrate	154	2440
Stannic phosphides	139	1433
Stibine	119	2676
Straw, wet, damp or contaminated with oil	133	1327
Strontium arsenite	151	1691
Strontium chlorate	143	1506
Strontium nitrate	140	1507
Strontium perchlorate	140	1508
Strontium peroxide	143	1509
Strontium phosphide	139	2013
Strychnine	151	1692
Strychnine salts	151	1692
Styrene monomer, stabilized	128P	2055
Substituted nitrophenol pesticide, liquid, flammable, poisonous	131	2780
Substituted nitrophenol pesticide, liquid, flammable, toxic	131	2780
Substituted nitrophenol pesticide, liquid, poisonous	153	3014
Substituted nitrophenol pesticide, liquid, poisonous, flammable	131	3013
Substituted nitrophenol pesticide, liquid, toxic	153	3014
Substituted nitrophenol pesticide, liquid, toxic, flammable	131	3013
Substituted nitrophenol pesticide, solid, poisonous	153	2779
Substituted nitrophenol pesticide, solid, toxic	153	2779
Sulfamic acid	154	2967
Sulfur	133	1350
Sulfur, molten	133	2448
Sulfur chlorides	137	1828
Sulfur dioxide	125	1079
Sulfur hexafluoride	126	1080
Sulfuric acid	137	1830
Sulfuric acid, fuming	137	1831
Sulfuric acid, spent	137	1832
Sulfuric acid, with more than 51% acid	137	1830
Sulfuric acid, with not more than 51% acid	157	2796
Sulfuric acid and Hydrofluoric acid mixture	157	1786
Sulfurous acid	154	1833
Sulfur tetrafluoride	125	2418
Sulfur trioxide, stabilized	137	1829
Sulfuryl chloride	137	1834
Sulfuryl fluoride	123	2191
Sulphamic acid	154	2967
Sulphur	133	1350
Sulphur, molten	133	2448
Sulphur chlorides	137	1828
Sulphur dioxide	125	1079
Sulphur hexafluoride	126	1080
Sulphuric acid	137	1830
Sulphuric acid, fuming	137	1831

Name of Material	Guide No.	ID No.
Sulphuric acid, spent	137	1832
Sulphuric acid, with more than 51% acid	137	1830
Sulphuric acid, with not more than 51% acid	157	2796
Sulphuric acid and Hydrofluoric acid mixture	157	1786
Sulphurous acid	154	1833
Sulphur tetrafluoride	125	2418
Sulphur trioxide, stabilized	137	1829
Sulphuryl chloride	137	1834
Sulphuryl fluoride	123	2191
Tabun	153	——
Tars, liquid	130	1999
Tear gas candles	159	1700
Tear gas devices	159	1693
Tear gas grenades	159	1700
Tear gas substance, liquid, n.o.s.	159	1693
Tear gas substance, solid, n.o.s.	159	3448
Tellurium compound, n.o.s.	151	3284
Tellurium hexafluoride	125	2195
Terpene hydrocarbons, n.o.s.	128	2319
Terpinolene	128	2541
Tetrabromoethane	159	2504
1,1,2,2-Tetrachloroethane	151	1702
Tetrachloroethylene	160	1897
Tetraethyl dithiopyrophosphate	153	1704
Tetraethylenepentamine	153	2320
Tetraethyl silicate	129	1292
1,1,1,2-Tetrafluoroethane	126	3159
Tetrafluoroethane and Ethylene oxide mixture, with not more than 5.6% Ethylene oxide	126	3299
Tetrafluoroethylene, stabilized	116P	1081
Tetrafluoromethane	126	1982
Tetrafluoromethane, compressed	126	1982
1,2,3,6-Tetrahydrobenzaldehyde	129	2498
Tetrahydrofuran	127	2056
Tetrahydrofurfurylamine	129	2943
Tetrahydrophthalic anhydrides	156	2698
1,2,3,6-Tetrahydropyridine	129	2410
Tetrahydrothiophene	130	2412
Tetramethylammonium hydroxide, solid	153	3423
Tetramethylammonium hydroxide, solution	153	1835
Tetramethylsilane	130	2749
Tetranitromethane	143	1510
Tetrapropyl orthotitanate	128	2413
Textile waste, wet	133	1857
Thallium chlorate	141	2573
Thallium compound, n.o.s.	151	1707
Thallium nitrate	141	2727
4-Thiapentanal	152	2785
Thickened GD	153	——
Thioacetic acid	129	2436
Thiocarbamate pesticide, liquid, flammable, poisonous	131	2772
Thiocarbamate pesticide, liquid, flammable, toxic	131	2772
Thiocarbamate pesticide, liquid, poisonous	151	3006
Thiocarbamate pesticide, liquid, poisonous, flammable	131	3005
Thiocarbamate pesticide, liquid, toxic	151	3006

Name of Material	Guide No.	ID No.
Thiocarbamate pesticide, liquid, toxic, flammable	131	3005
Thiocarbamate pesticide, solid, poisonous	151	2771
Thiocarbamate pesticide, solid, toxic	151	2771
Thioglycol	153	2966
Thioglycolic acid	153	1940
Thiolactic acid	153	2936
Thionyl chloride	137	1836
Thiophene	130	2414
Thiophosgene	157	2474
Thiophosphoryl chloride	157	1837
Thiourea dioxide	135	3341
Tinctures, medicinal	127	1293
Tin tetrachloride	137	1827
Titanium disulfide	135	3174
Titanium disulphide	135	3174
Titanium hydride	170	1871
Titanium powder, dry	135	2546
Titanium powder, wetted with not less than 25% water	170	1352
Titanium sponge granules	170	2878
Titanium sponge powders	170	2878
Titanium tetrachloride	137	1838
Titanium trichloride, pyrophoric	135	2441
Titanium trichloride mixture	157	2869
Titanium trichloride mixture, pyrophoric	135	2441
TNT, wetted with not less than 10% water	113	3366
TNT, wetted with not less than 30% water	113	1356
Toluene	130	1294
2,4-Toluenediamine, solid	151	1709
2,4-Toluenediamine, solution	151	3418
Toluene diisocyanate	156	2078
Toluidines, liquid	153	1708
Toluidines, solid	153	3451
2,4-Toluylenediamine, solid	151	1709
2,4-Toluylenediamine, solution	151	3418
Toxic by inhalation liquid, corrosive, flammable, n.o.s. (Inhalation Hazard Zone A)	131	3492
Toxic by inhalation liquid, corrosive, flammable, n.o.s. (Inhalation Hazard Zone B)	131	3493
Toxic by inhalation liquid, corrosive, n.o.s. (Inhalation Hazard Zone A)	154	3389
Toxic by inhalation liquid, corrosive, n.o.s. (Inhalation Hazard Zone B)	154	3390
Toxic by inhalation liquid, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)	131	3488
Toxic by inhalation liquid, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)	131	3489
Toxic by inhalation liquid, flammable, n.o.s. (Inhalation Hazard Zone A)	131	3383
Toxic by inhalation liquid, flammable, n.o.s. (Inhalation Hazard Zone B)	131	3384
Toxic by inhalation liquid, n.o.s. (Inhalation Hazard Zone A)	151	3381
Toxic by inhalation liquid, n.o.s. (Inhalation Hazard Zone B)	151	3382
Toxic by inhalation liquid, oxidizing, n.o.s. (Inhalation Hazard Zone A)	142	3387
Toxic by inhalation liquid, oxidizing, n.o.s. (Inhalation Hazard Zone B)	142	3388

Name of Material	Guide No.	ID No.
Toxic by inhalation liquid, water-reactive, flammable, n.o.s. (Inhalation Hazard Zone A)	155	3490
Toxic by inhalation liquid, water-reactive, flammable, n.o.s. (Inhalation Hazard Zone B)	155	3491
Toxic by inhalation liquid, water-reactive, n.o.s. (Inhalation Hazard Zone A)	139	3385
Toxic by inhalation liquid, water-reactive, n.o.s. (Inhalation Hazard Zone B)	139	3386
Toxic liquid, corrosive, inorganic, n.o.s.	154	3289
Toxic liquid, corrosive, organic, n.o.s.	154	2927
Toxic liquid, flammable, organic, n.o.s.	131	2929
Toxic liquid, inorganic, n.o.s.	151	3287
Toxic liquid, organic, n.o.s.	153	2810
Toxic liquid, oxidizing, n.o.s.	142	3122
Toxic liquid, water-reactive, n.o.s.	139	3123
Toxic solid, corrosive, inorganic, n.o.s.	154	3290
Toxic solid, corrosive, organic, n.o.s.	154	2928
Toxic solid, flammable, inorganic, n.o.s.	134	3535
Toxic solid, flammable, organic, n.o.s.	134	2930
Toxic solid, inorganic, n.o.s.	151	3288
Toxic solid, organic, n.o.s.	154	2811
Toxic solid, oxidizing, n.o.s.	141	3086
Toxic solid, self-heating, n.o.s.	136	3124
Toxic solid, water-reactive, n.o.s.	139	3125
Toxins	153	——
Toxins, extracted from living sources, liquid, n.o.s.	153	3172
Toxins, extracted from living sources, solid, n.o.s.	153	3462
Triallylamine	132	2610
Triallyl borate	156	2609
Triazine pesticide, liquid, flammable, poisonous	131	2764
Triazine pesticide, liquid, flammable, toxic	131	2764
Triazine pesticide, liquid, poisonous	151	2998
Triazine pesticide, liquid, poisonous, flammable	131	2997
Triazine pesticide, liquid, toxic	151	2998
Triazine pesticide, liquid, toxic, flammable	131	2997
Triazine pesticide, solid, poisonous	151	2763
Triazine pesticide, solid, toxic	151	2763
Tributylamine	153	2542
Tributylphosphane	135	3254
Trichloroacetic acid	153	1839
Trichloroacetic acid, solution	153	2564
Trichloroacetyl chloride	156	2442
Trichlorobenzenes, liquid	153	2321
Trichlorobutene	152	2322
1,1,1-Trichloroethane	160	2831
Trichloroethylene	160	1710
Trichloroisocyanuric acid, dry	140	2468
Trichlorosilane	139	1295
Tricresyl phosphate	151	2574
Triethylamine	132	1296
Triethylenetetramine	153	2259

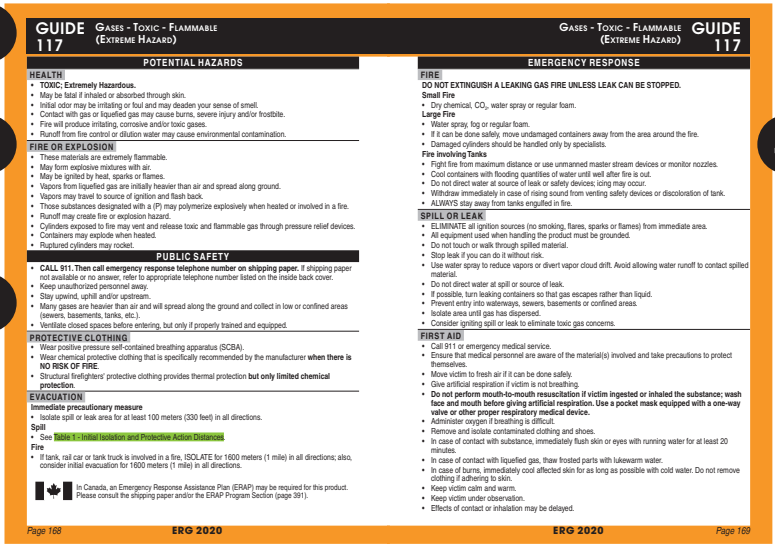
Name of Material	Guide No.	ID No.
Triethyl phosphite	130	2323
Trifluoroacetic acid	154	2699
Trifluoroacetyl chloride	125	3057
Trifluorochloroethylene, stabilized	119P	1082
1,1,1-Trifluoroethane	115	2035
Trifluoromethane	126	1984
Trifluoromethane, refrigerated liquid	120	3136
Trifluoromethane and Chlorotrifluoromethane azeotropic mixture with approximately 60% Chlorotrifluoromethane	126	2599
2-Trifluoromethylaniline	153	2942
3-Trifluoromethylaniline	153	2948
Triisobutylene	128	2324
Triisopropyl borate	129	2616
Trimethoxysilane	132	9269
Trimethylacetyl chloride	131	2438
Trimethylamine, anhydrous	118	1083
Trimethylamine, aqueous solution	132	1297
1,3,5-Trimethylbenzene	129	2325
Trimethyl borate	129	2416
Trimethylchlorosilane	155	1298
Trimethylcyclohexylamine	153	2326
Trimethylhexamethylenediamines	153	2327
Trimethylhexamethylene diisocyanate	156	2328
Trimethyl phosphite	130	2329
Trinitrobenzene, wetted with not less than 10% water	113	3367
Trinitrobenzene, wetted with not less than 30% water	113	1354
Trinitrobenzoic acid, wetted with not less than 10% water	113	3368
Trinitrobenzoic acid, wetted with not less than 30% water	113	1355
Trinitrochlorobenzene, wetted with not less than 10% water	113	3365
Trinitrophenol, wetted with not less than 10% water	113	3364
Trinitrophenol, wetted with not less than 30% water	113	1344
Trinitrotoluene, wetted with not less than 10% water	113	3366
Trinitrotoluene, wetted with not less than 30% water	113	1356
Tripropylamine	132	2260
Tripropylene	128	2057
Tris-(1-aziridinyl)phosphine oxide, solution	152	2501
Tungsten hexafluoride	125	2196
Turpentine	128	1299
Turpentine substitute	128	1300
Undecane	128	2330
Uranium hexafluoride, radioactive material, excepted package, less than 0.1 kg per package, non-fissile or fissile-excepted	166	3507
Uranium hexafluoride, radioactive material, fissile	166	2977
Uranium hexafluoride, radioactive material, non fissile or fissile-excepted	166	2978
Urea hydrogen peroxide	140	1511
Urea nitrate, wetted with not less than 10% water	113	3370
Urea nitrate, wetted with not less than 20% water	113	1357
Valeraldehyde	129	2058
Valeryl chloride	132	2502

Name of Material	Guide No.	ID No.
Vanadium compound, n.o.s.	**151**	3285
Vanadium oxytrichloride	**137**	2443
Vanadium pentoxide	**151**	2862
Vanadium tetrachloride	**137**	2444
Vanadium trichloride	**157**	2475
Vanadyl sulfate	**151**	2931
Vanadyl sulphate	**151**	2931
Vehicle, flammable gas powered	**115**	3166
Vehicle, flammable liquid powered	**128**	3166
Vehicle, fuel cell, flammable gas powered	**115**	3166
Vehicle, fuel cell, flammable liquid powered	**128**	3166
Vinyl acetate, stabilized	**129P**	1301
Vinyl bromide, stabilized	**116P**	1085
Vinyl butyrate, stabilized	**129P**	2838
Vinyl chloride, stabilized	**116P**	1086
Vinyl chloroacetate	**155**	2589
Vinyl ethyl ether, stabilized	**127P**	1302
Vinyl fluoride, stabilized	**116P**	1860
Vinylidene chloride, stabilized	**130P**	1303
Vinyl isobutyl ether, stabilized	**127P**	1304
Vinyl methyl ether, stabilized	**116P**	1087
Vinylpyridines, stabilized	**131P**	3073
Vinyltoluenes, stabilized	**130P**	2618
Vinyltrichlorosilane	**155P**	1305
Vinyltrichlorosilane, stabilized	**155P**	1305
VX	**153**	——
Water-reactive liquid, corrosive, n.o.s.	**138**	3129
Water-reactive liquid, n.o.s.	**138**	3148
Water-reactive liquid, poisonous, n.o.s.	**139**	3130
Water-reactive liquid, toxic, n.o.s.	**139**	3130
Water-reactive solid, corrosive, n.o.s.	**138**	3131
Water-reactive solid, flammable, n.o.s.	**138**	3132
Water-reactive solid, n.o.s.	**138**	2813
Water-reactive solid, oxidizing, n.o.s.	**138**	3133
Water-reactive solid, poisonous, n.o.s.	**139**	3134
Water-reactive solid, self-heating, n.o.s.	**138**	3135
Water-reactive solid, toxic, n.o.s.	**139**	3134
Wheelchair, electric, with batteries	**154**	3171
White asbestos	**171**	2590
White phosphorus, dry or under water or in solution	**136**	1381
White phosphorus, molten	**136**	2447
Wood preservatives, liquid	**129**	1306
Wool waste, wet	**133**	1387
Xanthates	**135**	3342
Xenon	**120**	2036
Xenon, compressed	**120**	2036
Xenon, refrigerated liquid (cryogenic liquid)	**120**	2591
Xylenes	**130**	1307
Xylenols, liquid	**153**	3430
Xylenols, solid	**153**	2261
Xylidines, liquid	**153**	1711
Xylidines, solid	**153**	3452
Xylyl bromide, liquid	**152**	1701

Name of Material	Guide No.	ID No.
Xylyl bromide, solid	152	3417
Yellow phosphorus, dry or under water or in solution	136	1381
Zinc ammonium nitrite	140	1512
Zinc arsenate	151	1712
Zinc arsenate and Zinc arsenite mixture	151	1712
Zinc arsenite	151	1712
Zinc arsenite and Zinc arsenate mixture	151	1712
Zinc ashes	138	1435
Zinc bromate	140	2469
Zinc chlorate	140	1513
Zinc chloride, anhydrous	154	2331
Zinc chloride, solution	154	1840
Zinc cyanide	151	1713
Zinc dithionite	171	1931
Zinc dross	138	1435
Zinc dust	138	1436
Zinc fluorosilicate	151	2855
Zinc hydrosulfite	171	1931
Zinc hydrosulphite	171	1931
Zinc nitrate	140	1514
Zinc permanganate	140	1515
Zinc peroxide	143	1516
Zinc phosphide	139	1714
Zinc powder	138	1436
Zinc residue	138	1435
Zinc resinate	133	2714
Zinc silicofluoride	151	2855
Zinc skimmings	138	1435
Zirconium, dry, coiled wire, finished metal sheets or strip	170	2858
Zirconium, dry, finished sheets, strips or coiled wire	135	2009
Zirconium hydride	138	1437
Zirconium nitrate	140	2728
Zirconium picramate, wetted with not less than 20% water	113	1517
Zirconium powder, dry	135	2008
Zirconium powder, wetted with not less than 25% water	170	1358
Zirconium scrap	135	1932
Zirconium suspended in a flammable liquid	170	1308
Zirconium suspended in a liquid (flammable)	170	1308
Zirconium tetrachloride	137	2503

NOTES

HOW TO USE THE ORANGE GUIDES



GUIDE 117 GASES - TOXIC - FLAMMABLE (EXTREME HAZARD)

POTENTIAL HAZARDS

HEALTH
- **TOXIC; Extremely Hazardous.**
- May be fatal if inhaled or absorbed through skin.
- Initial odor may be irritating or foul and may deaden your sense of smell.
- Contact with gas or liquefied gas may cause burns, severe injury and/or frostbite.
- Fire will produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may cause environmental contamination.

FIRE OR EXPLOSION
- These materials are extremely flammable.
- May form explosive mixtures with air.
- May be ignited by heat, sparks or flames.
- Vapors from liquefied gas are initially heavier than air and spread along ground.
- Vapors may travel to source of ignition and flash back.
- Those substances designated with a (P) may polymerize explosively when heated or involved in a fire.
- Runoff may create fire or explosion hazard.
- Cylinders exposed to fire may vent and release toxic and flammable gas through pressure relief devices.
- Containers may explode when heated.
- Ruptured cylinders may rocket.

PUBLIC SAFETY
- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Many gases are heavier than air and will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING
- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE.**
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection.**

EVACUATION

Immediate precautionary measure
- Isolate spill or leak area for at least 100 meters (330 feet) in all directions.

Spill
- See Table 1 - Initial Isolation and Protective Action Distances.

Fire
- If tank, rail car or tank truck is involved in a fire, ISOLATE for 1600 meters (1 mile) in all directions; also, consider initial evacuation for 1600 meters (1 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 391).

Page 168 ERG 2020

GASES - TOXIC - FLAMMABLE (EXTREME HAZARD) GUIDE 117

EMERGENCY RESPONSE

FIRE

DO NOT EXTINGUISH A LEAKING GAS FIRE UNLESS LEAK CAN BE STOPPED.

Small Fire
- Dry chemical, CO_2, water spray or regular foam.

Large Fire
- Water spray, fog or regular foam.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Damaged cylinders should be handled only by specialists.

Fire involving Tanks
- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Do not direct water at source of leak or safety devices; icing may occur.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK
- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- Do not direct water at spill or source of leak.
- If possible, turn leaking containers so that gas escapes rather than liquid.
- Prevent entry into waterways, sewers, basements or confined areas.
- Isolate area until gas has dispersed.
- Consider igniting spill or leak to eliminate toxic gas concerns.

FIRST AID
- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- In case of contact with liquefied gas, thaw frosted parts with lukewarm water.
- In case of burns, immediately cool affected skin for as long as possible with cold water. Do not remove clothing if adhering to skin.
- Keep victim calm and warm.
- Keep victim under observation.
- Effects of contact or inhalation may be delayed.

ERG 2020 Page 169

1 2 3 4

1 GUIDE NUMBER AND TITLE

- The guide title identifies the general hazards associated with the materials in this Guide.

2 POTENTIAL HAZARDS

- Emergency responders should consult this section first!
- Describes the material hazard in terms of **FIRE OR EXPLOSION** and **HEALTH** effects upon exposure.
- The primary potential hazard is listed first.
- Allows the responders to make decisions to protect the emergency response team, and the surrounding population.

3 PUBLIC SAFETY

- This section is divided into three subsections:
  - **General Information:** describes initial precautionary measures to be taken by those first on the scene.
  - **PROTECTIVE CLOTHING:** provides general guidance on personal protective equipment requirements including respiratory protection. The protective clothing information is general and correct selection is situation dependent, after considering the physical and chemical properties of the material, weather conditions, spill versus fire, topography, etc.
  - **EVACUATION:** suggests protective distances for immediate precautionary measures defined for small and large spills, including suggested guidance for conditions where fire is present or likely (potential fragmentation hazard).
    - The term "isolate" indicates a zone of no entry that applies to the public and first responders who are not equipped, trained, and prepared to mitigate the incident.
    - The term "evacuate" indicates people should be removed from inside this zone, if it can be done safely. If removal is too risky, sheltering-in-place can also be considered in this zone. Evacuation aims to protect as many people as possible, and applies mainly to the public.
- Materials highlighted in green in the yellow-bordered and blue-bordered pages direct the reader to consult Table 1, detailing specific response distances for toxic inhalation hazard materials, water-reactive materials and chemical warfare agents (green-bordered pages).



If a Canadian flag appears in this section, and the incident is located in Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product.

4 EMERGENCY RESPONSE

- This section is divided into three subsections:
  - **FIRE:** provides extinguishing procedures for **Small Fire**, **Large Fire**, and/or **Fire Involving Tanks or Car/Trailer Loads**
  - **SPILL OR LEAK:** includes general recommendations, and may describe the response procedure for **Small Spill** and **Large Spill**
  - **FIRST AID:** provides general guidance prior to seeking expert medical care.

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- May explode from heat, shock, friction or contamination.
- May react violently or explosively on contact with air, water or foam.
- May be ignited by heat, sparks or flames.
- Vapors may travel to source of ignition and flash back.
- Containers may explode when heated.
- Ruptured cylinders may rocket.

HEALTH

- Inhalation, ingestion or contact with substance may cause severe injury, infection, disease or death.
- High concentration of gas may cause asphyxiation without warning.
- Contact may cause burns to skin and eyes.
- Fire or contact with water may produce irritating, toxic and/or corrosive gases.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper**. If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 100 meters (330 feet) in all directions.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

EMERGENCY RESPONSE

FIRE

CAUTION: Material may react with extinguishing agent.

Small Fire

- Dry chemical, CO_2, water spray or regular foam.

Large Fire

- Water spray, fog or regular foam.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks

- Cool containers with flooding quantities of water until well after fire is out.
- Do not get water inside containers.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- Do not touch or walk through spilled material.
- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Keep combustibles (wood, paper, oil, etc.) away from spilled material.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- Prevent entry into waterways, sewers, basements or confined areas.

Small Spill

- Pick up with sand or other non-combustible absorbent material and place into containers for later disposal.

Large Spill

- Dike far ahead of liquid spill for later disposal.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Shower and wash with soap and water.
- Keep victim calm and warm.
- Effects of exposure (inhalation, ingestion or skin contact) to substance may be delayed.

GUIDE 112 Explosives* - Division 1.1, 1.2, 1.3 or 1.5

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- **MAY EXPLODE AND THROW FRAGMENTS 1600 METERS (1 MILE) OR MORE IF FIRE REACHES CARGO.**
- **For information on "Compatibility Group" letters, refer to Glossary section.**

HEALTH

- Fire may produce irritating, corrosive and/or toxic gases.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Move people out of line of sight of the scene and away from windows.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area immediately for at least 500 meters (1/3 mile) in all directions.

Large Spill

- **Consider initial evacuation for 800 meters (1/2 mile) in all directions.**

Fire

- If rail car or trailer is involved in a fire, ISOLATE for 1600 meters (1 mile) in all directions; also, initiate evacuation including emergency responders for 1600 meters (1 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

*** For information on "Compatibility Group" Letters, refer to the Glossary section.**

EMERGENCY RESPONSE

FIRE

CARGO Fire

- **DO NOT fight fire when fire reaches cargo! Cargo may EXPLODE!**
- Stop all traffic and clear the area for at least 1600 meters (1 mile) in all directions and let burn.
- **Do not move cargo or vehicle if cargo has been exposed to heat.**

TIRE or VEHICLE Fire

- **Use plenty of water - FLOOD it! If water is not available, use CO_2, dry chemical or dirt.**
- If possible, and WITHOUT RISK, use unmanned master stream devices or monitor nozzles from maximum distance to prevent fire from spreading to cargo area.
- Pay special attention to tire fires as re-ignition may occur. Stand by, at a safe distance, with extinguisher ready for possible re-ignition.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch or walk through spilled material.
- DO NOT OPERATE RADIO TRANSMITTERS WITHIN 100 METERS (330 FEET) OF ELECTRIC DETONATORS.
- **DO NOT CLEAN-UP OR DISPOSE OF, EXCEPT UNDER SUPERVISION OF A SPECIALIST.**

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.

*** FOR INFORMATION ON "COMPATIBILITY GROUP" LETTERS, REFER TO THE GLOSSARY SECTION.**

GUIDE 113 Flammable Materials (Wet/Desensitized Explosive)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- Flammable/combustible material.
- May be ignited by heat, sparks or flames.
- **DRIED OUT material may explode if exposed to heat, flame, friction or shock; treat as an explosive (GUIDE 112).**
- **Keep material wet with water or treat as an explosive (GUIDE 112).**
- Runoff to sewer may create fire or explosion hazard.

HEALTH

- **Some are toxic** and may be fatal if inhaled, ingested or absorbed through skin. Specifically, Dinitrophenol, wetted (UN1320); Dinitrophenolates, wetted (UN1321), Sodium dinitro-o-cresolate, wetted (UN1348); and Barium azide, wetted (UN1571) are known to be toxic.
- Contact may cause burns to skin and eyes.
- Fire may produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area immediately for at least 100 meters (330 feet) in all directions.

Large Spill

- **Consider initial evacuation for 500 meters (1/3 mile) in all directions.**

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

CARGO Fire

- **DO NOT fight fire when fire reaches cargo! Cargo may EXPLODE!**
- Stop all traffic and clear the area for at least 1600 meters (1 mile) in all directions and let burn.
- **Do not move cargo or vehicle if cargo has been exposed to heat.**

TIRE or VEHICLE Fire

- **Use plenty of water - FLOOD it! If water is not available, use CO_2, dry chemical or dirt.**
- If possible, and WITHOUT RISK, use unmanned master stream devices or monitor nozzles from maximum distance to prevent fire from spreading to cargo area.
- Pay special attention to tire fires as re-ignition may occur. Stand by, at a safe distance, with extinguisher ready for possible re-ignition.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch or walk through spilled material.

Small Spill

- Flush area with large amounts of water.

Large Spill

- Wet down with water and dike for later disposal.
- KEEP "WETTED" PRODUCT WET BY SLOWLY ADDING FLOODING QUANTITIES OF WATER.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.

GUIDE 114 EXPLOSIVES* - DIVISION 1.4 OR 1.6

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- **MAY EXPLODE AND THROW FRAGMENTS 800 METERS (1/2 MILE) OR MORE IF FIRE REACHES CARGO.**
- **For information on "Compatibility Group" letters, refer to Glossary section.**

HEALTH

- Fire may produce irritating, corrosive and/or toxic gases.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Move people out of line of sight of the scene and away from windows.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area immediately for at least 100 meters (330 feet) in all directions.

Large Spill

- **Consider initial evacuation for 250 meters (800 feet) in all directions.**

Fire

- If rail car or trailer is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also initiate evacuation including emergency responders for 800 meters (1/2 mile) in all directions.
- If fire threatens cargo area containing packages bearing the 1.4S label or packages containing material classified as 1.4S, consider isolating at least 15 meters (50 feet) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

*** FOR INFORMATION ON "COMPATIBILITY GROUP" LETTERS, REFER TO THE GLOSSARY SECTION.**

EMERGENCY RESPONSE

FIRE

CARGO Fire

- **DO NOT fight fire when fire reaches cargo! Cargo may EXPLODE!**
- Stop all traffic and clear the area for at least 800 meters (1/2 mile) in all directions and let burn.
- **Do not move cargo or vehicle if cargo has been exposed to heat.**

TIRE or VEHICLE Fire

- **Use plenty of water - FLOOD it! If water is not available, use CO_2, dry chemical or dirt.**
- If possible, and WITHOUT RISK, use unmanned master stream devices or monitor nozzles from maximum distance to prevent fire from spreading to cargo area.
- Pay special attention to tire fires as re-ignition may occur. Stand by, at a safe distance, with extinguisher ready for possible re-ignition.

CLASS 1.4S Fire

- Packages bearing the 1.4S label or packages containing material classified as 1.4S are designed or packaged in such a manner that when involved in a fire, they may burn vigorously with localized detonations and projection of fragments.
- Effects are usually confined to immediate vicinity of packages.
- Fight fire with normal precautions from a reasonable distance.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch or walk through spilled material.
- DO NOT OPERATE RADIO TRANSMITTERS WITHIN 100 METERS (330 FEET) OF ELECTRIC DETONATORS.
- **DO NOT CLEAN-UP OR DISPOSE OF, EXCEPT UNDER SUPERVISION OF A SPECIALIST.**

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.

*** FOR INFORMATION ON "COMPATIBILITY GROUP" LETTERS, REFER TO THE GLOSSARY SECTION.**

GUIDE 115 Gases - Flammable (Including Refrigerated Liquids)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- **EXTREMELY FLAMMABLE.**
- Will be easily ignited by heat, sparks or flames.
- Will form explosive mixtures with air.
- Vapors from liquefied gas are initially heavier than air and spread along ground.

CAUTION: Hydrogen (UN1049), Deuterium (UN1957), Hydrogen, refrigerated liquid (UN1966), Methane (UN1971) and Hydrogen and Methane mixture, compressed (UN2034) are lighter than air and will rise. Hydrogen and Deuterium fires are difficult to detect since they burn with an invisible flame. Use an alternate method of detection (thermal camera, broom handle, etc.)

- Vapors may travel to source of ignition and flash back.
- Cylinders exposed to fire may vent and release flammable gas through pressure relief devices.
- Containers may explode when heated.
- Ruptured cylinders may rocket.

HEALTH

- Vapors may cause dizziness or asphyxiation without warning.
- Some may be irritating if inhaled at high concentrations.
- Contact with gas or liquefied gas may cause burns, severe injury and/or frostbite.
- Fire may produce irritating and/or toxic gases.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Many gases are heavier than air and will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.
- Always wear thermal protective clothing when handling refrigerated/cryogenic liquids.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 100 meters (330 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 800 meters (1/2 mile).

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 1600 meters (1 mile) in all directions; also, consider initial evacuation for 1600 meters (1 mile) in all directions.
- In fires involving Liquefied Petroleum Gases (LPG) (UN1075), Butane (UN1011), Butylene (UN1012), Isobutylene (UN1055), Propylene (UN1077), Isobutane (UN1969), and Propane (UN1978), also refer to BLEVE – SAFETY PRECAUTIONS (Page 366).



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- **DO NOT EXTINGUISH A LEAKING GAS FIRE UNLESS LEAK CAN BE STOPPED.**

CAUTION: Hydrogen (UN1049), Deuterium (UN1957), Hydrogen, refrigerated liquid (UN1966) and Hydrogen and Methane mixture, compressed (UN2034) will burn with an invisible flame. Use an alternate method of detection (thermal camera, broom handle, etc.)

Small Fire

- Dry chemical or CO_2.

Large Fire

- Water spray or fog.
- If it can be done safely, move undamaged containers away from the area around the fire.

CAUTION: For **LNG - Liquefied natural gas (UN1972)** pool fires, DO NOT USE water. Use dry chemical or high-expansion foam.

Fire Involving Tanks

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Do not direct water at source of leak or safety devices; icing may occur.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- If possible, turn leaking containers so that gas escapes rather than liquid.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- Do not direct water at spill or source of leak.

CAUTION: For **LNG - Liquefied natural gas (UN1972)**, DO NOT apply water, regular or alcohol-resistant foam directly on spill. Use a high-expansion foam if available to reduce vapors.

- Prevent spreading of vapors through sewers, ventilation systems and confined areas.
- Isolate area until gas has dispersed.

CAUTION: When in contact with refrigerated/cryogenic liquids, many materials become brittle and are likely to break without warning.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- Clothing frozen to the skin should be thawed before being removed.
- In case of contact with liquefied gas, thaw frosted parts with lukewarm water.
- In case of burns, immediately cool affected skin for as long as possible with cold water. Do not remove clothing if adhering to skin. • Keep victim calm and warm.

GUIDE 116 Gases - Flammable (Unstable)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- **EXTREMELY FLAMMABLE.**
- Will be easily ignited by heat, sparks or flames.
- Will form explosive mixtures with air. Acetylene (UN1001, UN3374) may react explosively even in the absence of air.
- Silane (UN2203) will ignite spontaneously in air.
- Those substances designated with a **(P)** may polymerize explosively when heated or involved in a fire.
- Vapors from liquefied gas are initially heavier than air and spread along ground.
- Vapors may travel to source of ignition and flash back.
- Cylinders exposed to fire may vent and release flammable gas through pressure relief devices.
- Containers may explode when heated.
- Ruptured cylinders may rocket.

HEALTH

- Vapors may cause dizziness or asphyxiation without warning.
- Some may be toxic if inhaled at high concentrations.
- Contact with gas or liquefied gas may cause burns, severe injury and/or frostbite.
- Fire may produce irritating and/or toxic gases.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Many gases are heavier than air and will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 100 meters (330 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 800 meters (1/2 mile).

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 1600 meters (1 mile) in all directions; also, consider initial evacuation for 1600 meters (1 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- **DO NOT EXTINGUISH A LEAKING GAS FIRE UNLESS LEAK CAN BE STOPPED.**

Small Fire

- Dry chemical or CO_2.

Large Fire

- Water spray or fog.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Do not direct water at source of leak or safety devices; icing may occur.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Stop leak if you can do it without risk.
- Do not touch or walk through spilled material.
- Do not direct water at spill or source of leak.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- If possible, turn leaking containers so that gas escapes rather than liquid.
- Prevent entry into waterways, sewers, basements or confined areas.
- Isolate area until gas has dispersed.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with liquefied gas, thaw frosted parts with lukewarm water.
- In case of burns, immediately cool affected skin for as long as possible with cold water. Do not remove clothing if adhering to skin.
- Keep victim calm and warm.

GUIDE 117 Gases - Toxic - Flammable (Extreme Hazard)

POTENTIAL HAZARDS

HEALTH

- **TOXIC; Extremely Hazardous.**
- May be fatal if inhaled or absorbed through skin.
- Initial odor may be irritating or foul and may deaden your sense of smell.
- Contact with gas or liquefied gas may cause burns, severe injury and/or frostbite.
- Fire will produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may cause environmental contamination.

FIRE OR EXPLOSION

- These materials are extremely flammable.
- May form explosive mixtures with air.
- May be ignited by heat, sparks or flames.
- Vapors from liquefied gas are initially heavier than air and spread along ground.
- Vapors may travel to source of ignition and flash back.
- Those substances designated with a **(P)** may polymerize explosively when heated or involved in a fire.
- Runoff may create fire or explosion hazard.
- Cylinders exposed to fire may vent and release toxic and flammable gas through pressure relief devices.
- Containers may explode when heated.
- Ruptured cylinders may rocket.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Many gases are heavier than air and will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 100 meters (330 feet) in all directions.

Spill

- See Table 1 - Initial Isolation and Protective Action Distances.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 1600 meters (1 mile) in all directions; also, consider initial evacuation for 1600 meters (1 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- **DO NOT EXTINGUISH A LEAKING GAS FIRE UNLESS LEAK CAN BE STOPPED.**

Small Fire

- Dry chemical, CO_2, water spray or regular foam.

Large Fire

- Water spray, fog or regular foam.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Damaged cylinders should be handled only by specialists.

Fire Involving Tanks

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Do not direct water at source of leak or safety devices; icing may occur.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- Do not direct water at spill or source of leak.
- If possible, turn leaking containers so that gas escapes rather than liquid.
- Prevent entry into waterways, sewers, basements or confined areas.
- Isolate area until gas has dispersed.
- Consider igniting spill or leak to eliminate toxic gas concerns.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- In case of contact with liquefied gas, thaw frosted parts with lukewarm water.
- In case of burns, immediately cool affected skin for as long as possible with cold water. Do not remove clothing if adhering to skin.
- Keep victim calm and warm.
- Keep victim under observation.
- Effects of contact or inhalation may be delayed.

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- **EXTREMELY FLAMMABLE.**
- May be ignited by heat, sparks or flames.
- May form explosive mixtures with air.
- Vapors from liquefied gas are initially heavier than air and spread along ground.
- Vapors may travel to source of ignition and flash back.
- Some of these materials may react violently with water.
- Cylinders exposed to fire may vent and release flammable gas through pressure relief devices.
- Containers may explode when heated.
- Ruptured cylinders may rocket.

HEALTH

- May cause toxic effects if inhaled.
- Vapors are extremely irritating.
- Contact with gas or liquefied gas may cause burns, severe injury and/or frostbite.
- Fire will produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Many gases are heavier than air and will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 100 meters (330 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 800 meters (1/2 mile).

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 1600 meters (1 mile) in all directions; also, consider initial evacuation for 1600 meters (1 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- **DO NOT EXTINGUISH A LEAKING GAS FIRE UNLESS LEAK CAN BE STOPPED.**

Small Fire

- Dry chemical or CO_2.

Large Fire

- Water spray, fog or regular foam.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Damaged cylinders should be handled only by specialists.

Fire Involving Tanks

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Do not direct water at source of leak or safety devices; icing may occur.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- If possible, turn leaking containers so that gas escapes rather than liquid.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- Do not direct water at spill or source of leak.
- Isolate area until gas has dispersed.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with liquefied gas, thaw frosted parts with lukewarm water.
- In case of burns, immediately cool affected skin for as long as possible with cold water. Do not remove clothing if adhering to skin.
- Keep victim calm and warm.
- Keep victim under observation.
- Effects of contact or inhalation may be delayed.

POTENTIAL HAZARDS

HEALTH

- **TOXIC; may be fatal if inhaled or absorbed through skin. Some may cause severe skin burns and eye damage.**
- Contact with gas or liquefied gas may cause burns, severe injury and/or frostbite.
- Fire will produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may cause environmental contamination.

FIRE OR EXPLOSION

- Flammable; may be ignited by heat, sparks or flames.
- May form explosive mixtures with air. Ethylene oxide (UN1040) may react explosively even in the absence of air.
- Those substances designated with a **(P)** may polymerize explosively when heated or involved in a fire.
- Vapors from liquefied gas are initially heavier than air and spread along ground.
- Vapors may travel to source of ignition and flash back.
- Some of these materials may react violently with water.
- Cylinders exposed to fire may vent and release toxic and flammable gas through pressure relief devices.
- Containers may explode when heated.
- Ruptured cylinders may rocket.
- Runoff may create fire or explosion hazard.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Many gases are heavier than air and will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 100 meters (330 feet) in all directions.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 1600 meters (1 mile) in all directions; also, consider initial evacuation for 1600 meters (1 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- **DO NOT EXTINGUISH A LEAKING GAS FIRE UNLESS LEAK CAN BE STOPPED.**

Small Fire

- Dry chemical, CO_2, water spray or alcohol-resistant foam.

Large Fire

- Water spray, fog or alcohol-resistant foam.
- **FOR CHLOROSILANES, DO NOT USE WATER;** use AFFF alcohol-resistant medium-expansion foam.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Damaged cylinders should be handled only by specialists.

Fire Involving Tanks

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Do not direct water at source of leak or safety devices; icing may occur.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- Do not direct water at spill or source of leak.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- **FOR CHLOROSILANES**, use AFFF alcohol-resistant medium-expansion foam to reduce vapors.
- If possible, turn leaking containers so that gas escapes rather than liquid.
- Prevent entry into waterways, sewers, basements or confined areas.
- Isolate area until gas has dispersed.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- In case of contact with liquefied gas, thaw frosted parts with lukewarm water.
- In case of burns, immediately cool affected skin for as long as possible with cold water. Do not remove clothing if adhering to skin.
- Keep victim calm and warm.
- Keep victim under observation.
- Effects of contact or inhalation may be delayed.

GUIDE 120 Gases - Inert (Including Refrigerated Liquids)

POTENTIAL HAZARDS

HEALTH

- Vapors may cause dizziness or asphyxiation without warning.
- Vapors from liquefied gas are initially heavier than air and spread along ground.
- Contact with gas or liquefied gas may cause burns, severe injury and/or frostbite.

FIRE OR EXPLOSION

- **Non-flammable gases.**
- Containers may explode when heated.
- Ruptured cylinders may rocket.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Many gases are heavier than air and will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.
- Always wear thermal protective clothing when handling refrigerated/cryogenic liquids or solids.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 100 meters (330 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 100 meters (330 feet).

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

EMERGENCY RESPONSE

FIRE

- Use extinguishing agent suitable for type of surrounding fire.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Damaged cylinders should be handled only by specialists.

Fire Involving Tanks

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Do not direct water at source of leak or safety devices; icing may occur.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- Do not direct water at spill or source of leak.
- If possible, turn leaking containers so that gas escapes rather than liquid.
- Prevent entry into waterways, sewers, basements or confined areas.
- Allow substance to evaporate.
- Ventilate the area.

CAUTION: When in contact with refrigerated/cryogenic liquids, many materials become brittle and are likely to break without warning.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Clothing frozen to the skin should be thawed before being removed.
- In case of contact with liquefied gas, thaw frosted parts with lukewarm water.
- Keep victim calm and warm.

Page intentionally left blank

There are no materials that refer to this guide.

Page intentionally left blank

There are no materials that refer to this guide.

GUIDE 122 Gases - Oxidizing (Including Refrigerated Liquids)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- Substance does not burn but will support combustion.
- Some may react explosively with fuels.
- May ignite combustibles (wood, paper, oil, clothing, etc.).
- Vapors from liquefied gas are initially heavier than air and spread along ground.
- Runoff may create fire or explosion hazard.
- Containers may explode when heated.
- Ruptured cylinders may rocket.

HEALTH

- Vapors may cause dizziness or asphyxiation without warning.
- Contact with gas or liquefied gas may cause burns, severe injury and/or frostbite.
- Fire may produce irritating and/or toxic gases.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Many gases are heavier than air and will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.
- Always wear thermal protective clothing when handling refrigerated/cryogenic liquids.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 100 meters (330 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 500 meters (1/3 mile).

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- Use extinguishing agent suitable for type of surrounding fire.

Small Fire

- Dry chemical or CO_2.

Large Fire

- Water spray, fog or regular foam.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Damaged cylinders should be handled only by specialists.

Fire Involving Tanks

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Do not direct water at source of leak or safety devices; icing may occur.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- Keep combustibles (wood, paper, oil, etc.) away from spilled material.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- If possible, turn leaking containers so that gas escapes rather than liquid.
- Do not direct water at spill or source of leak.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- Prevent entry into waterways, sewers, basements or confined areas.
- Allow substance to evaporate.
- Isolate area until gas has dispersed.

CAUTION: When in contact with refrigerated/cryogenic liquids, many materials become brittle and are likely to break without warning.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- Clothing frozen to the skin should be thawed before being removed.
- In case of contact with liquefied gas, thaw frosted parts with lukewarm water.
- Keep victim calm and warm.

POTENTIAL HAZARDS

HEALTH

- **TOXIC; may be fatal if inhaled or absorbed through skin.**
- Vapors may be irritating and/or corrosive.
- Contact with gas or liquefied gas may cause burns, severe injury and/or frostbite.
- Fire will produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may cause environmental contamination.

FIRE OR EXPLOSION

- Some may burn but none ignite readily.
- Vapors from liquefied gas are initially heavier than air and spread along ground.
- Cylinders exposed to fire may vent and release toxic and/or corrosive gas through pressure relief devices.
- Containers may explode when heated.
- Ruptured cylinders may rocket.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Many gases are heavier than air and will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 100 meters (330 feet) in all directions.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

- Dry chemical or CO_2.

Large Fire

- Water spray, fog or regular foam.
- Do not get water inside containers.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Damaged cylinders should be handled only by specialists.

Fire Involving Tanks

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Do not direct water at source of leak or safety devices; icing may occur.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- If possible, turn leaking containers so that gas escapes rather than liquid.
- Prevent entry into waterways, sewers, basements or confined areas.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- Do not direct water at spill or source of leak.
- Isolate area until gas has dispersed.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with liquefied gas, thaw frosted parts with lukewarm water.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.
- Keep victim under observation.
- Effects of contact or inhalation may be delayed.

GUIDE 124 Gases - Toxic and/or Corrosive - Oxidizing

POTENTIAL HAZARDS

HEALTH

- **TOXIC; may be fatal if inhaled or absorbed through skin.**
- Fire will produce irritating, corrosive and/or toxic gases.
- Contact with gas or liquefied gas may cause burns, severe injury and/or frostbite.
- Runoff from fire control or dilution water may cause environmental contamination.

FIRE OR EXPLOSION

- Substance does not burn but will support combustion.
- Vapors from liquefied gas are initially heavier than air and spread along ground.
- These are strong oxidizers and will react vigorously or explosively with many materials including fuels.
- May ignite combustibles (wood, paper, oil, clothing, etc.).
- Some will react violently with air, moist air and/or water.
- Cylinders exposed to fire may vent and release toxic and/or corrosive gas through pressure relief devices.
- Containers may explode when heated.
- Ruptured cylinders may rocket.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Many gases are heavier than air and will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 100 meters (330 feet) in all directions.

Spill

- See Table 1 - Initial Isolation and Protective Action Distances.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

CAUTION: These materials do not burn but will support combustion. Some will react violently with water.

- Contain fire and let burn. If fire must be fought, water spray or fog is recommended.
- **Water only; no dry chemical, CO_2 or Halon®.**
- Do not get water inside containers.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Damaged cylinders should be handled only by specialists.

Fire Involving Tanks

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Do not direct water at source of leak or safety devices; icing may occur.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- Do not touch or walk through spilled material.
- Keep combustibles (wood, paper, oil, etc.) away from spilled material.
- Stop leak if you can do it without risk.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- Do not direct water at spill or source of leak.
- If possible, turn leaking containers so that gas escapes rather than liquid.
- Prevent entry into waterways, sewers, basements or confined areas.
- Isolate area until gas has dispersed.
- Ventilate the area.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Clothing frozen to the skin should be thawed before being removed.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.
- Keep victim under observation.
- Effects of contact or inhalation may be delayed.

GUIDE 125 Gases - Toxic and/or Corrosive

POTENTIAL HAZARDS

HEALTH

- **TOXIC; may be fatal if inhaled, ingested or absorbed through skin.**
- Vapors are extremely irritating and corrosive.
- Contact with gas or liquefied gas may cause burns, severe injury and/or frostbite.
- Fire will produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may cause environmental contamination.

FIRE OR EXPLOSION

- Some may burn but none ignite readily.
- Vapors from liquefied gas are initially heavier than air and spread along ground.
- Some of these materials may react violently with water.
- Cylinders exposed to fire may vent and release toxic and/or corrosive gas through pressure relief devices.
- Containers may explode when heated.
- Ruptured cylinders may rocket.
- For UN1005: Anhydrous ammonia, at high concentrations in confined spaces, presents a flammability risk if a source of ignition is introduced.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Many gases are heavier than air and will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 100 meters (330 feet) in all directions.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 1600 meters (1 mile) in all directions; also, consider initial evacuation for 1600 meters (1 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

- Dry chemical or CO_2.

Large Fire

- Water spray, fog or regular foam.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Do not get water inside containers.
- Damaged cylinders should be handled only by specialists.

Fire Involving Tanks

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Do not direct water at source of leak or safety devices; icing may occur.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- If possible, turn leaking containers so that gas escapes rather than liquid.
- Prevent entry into waterways, sewers, basements or confined areas.
- Do not direct water at spill or source of leak.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- Isolate area until gas has dispersed.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with liquefied gas, thaw frosted parts with lukewarm water.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- **In case of skin contact with hydrogen fluoride, anhydrous (UN1052)**, if calcium gluconate gel is available, rinse 5 minutes, then apply gel. Otherwise, continue rinsing until medical treatment is available.
- Keep victim calm and warm.
- Keep victim under observation.
- Effects of contact or inhalation may be delayed.

GUIDE 126 Gases - Compressed or Liquefied (Including Refrigerant Gases)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- Some may burn but none ignite readily.
- Containers may explode when heated.
- Ruptured cylinders may rocket.

CAUTION: Aerosols (UN1950) may contain a flammable propellant.

HEALTH

- Vapors may cause dizziness or asphyxiation without warning.
- Vapors from liquefied gas are initially heavier than air and spread along ground.
- Contact with gas or liquefied gas may cause burns, severe injury and/or frostbite.
- Fire may produce irritating, corrosive and/or toxic gases.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper**. If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Many gases are heavier than air and will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 100 meters (330 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 500 meters (1/3 mile).

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

EMERGENCY RESPONSE

FIRE

- Use extinguishing agent suitable for type of surrounding fire.

Small Fire

- Dry chemical or CO_2.

Large Fire

- Water spray, fog or regular foam.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Damaged cylinders should be handled only by specialists.

Fire Involving Tanks

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Do not direct water at source of leak or safety devices; icing may occur.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.
- Some of these materials, if spilled, may evaporate leaving a flammable residue.

SPILL OR LEAK

- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- Do not direct water at spill or source of leak.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- If possible, turn leaking containers so that gas escapes rather than liquid.
- Prevent entry into waterways, sewers, basements or confined areas.
- Allow substance to evaporate.
- Ventilate the area.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with liquefied gas, thaw frosted parts with lukewarm water.
- Keep victim calm and warm.

GUIDE 127 Flammable Liquids (Water-Miscible)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- **HIGHLY FLAMMABLE: Will be easily ignited by heat, sparks or flames.**

CAUTION: Ethanol (UN1170) can burn with an invisible flame. Use an alternate method of detection (thermal camera, broom handle, etc.)

- Vapors may form explosive mixtures with air.
- Vapors may travel to source of ignition and flash back.
- Most vapors are heavier than air. They will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Vapor explosion hazard indoors, outdoors or in sewers.
- Those substances designated with a **(P)** may polymerize explosively when heated or involved in a fire.
- Runoff to sewer may create fire or explosion hazard.
- Containers may explode when heated.
- Many liquids will float on water.

HEALTH

- Inhalation or contact with material may irritate or burn skin and eyes.
- Fire may produce irritating, corrosive and/or toxic gases.
- Vapors may cause dizziness or asphyxiation.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper**. If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 50 meters (150 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 300 meters (1000 feet).

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

CAUTION: The majority of these products have a very low flash point. Use of water spray when fighting fire may be inefficient.

CAUTION: For fire involving UN1170, UN1987 or UN3475, alcohol-resistant foam should be used.

CAUTION: Ethanol (UN1170) can burn with an invisible flame. Use an alternate method of detection (thermal camera, broom handle, etc.)

Small Fire

- Dry chemical, CO_2, water spray or alcohol-resistant foam.

Large Fire

- Water spray, fog or alcohol-resistant foam.
- Avoid aiming straight or solid streams directly onto the product.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- Prevent entry into waterways, sewers, basements or confined areas.
- A vapor-suppressing foam may be used to reduce vapors.
- Absorb or cover with dry earth, sand or other non-combustible material and transfer to containers.
- Use clean, non-sparking tools to collect absorbed material.

Large Spill

- Dike far ahead of liquid spill for later disposal.
- Water spray may reduce vapor, but may not prevent ignition in closed spaces.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Wash skin with soap and water.
- In case of burns, immediately cool affected skin for as long as possible with cold water. Do not remove clothing if adhering to skin.
- Keep victim calm and warm.

GUIDE 128 Flammable Liquids (Water-Immiscible)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- **HIGHLY FLAMMABLE: Will be easily ignited by heat, sparks or flames.**
- Vapors may form explosive mixtures with air.
- Vapors may travel to source of ignition and flash back.
- Most vapors are heavier than air. They will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Vapor explosion hazard indoors, outdoors or in sewers.
- Those substances designated with a **(P)** may polymerize explosively when heated or involved in a fire.
- Runoff to sewer may create fire or explosion hazard.
- Containers may explode when heated.
- Many liquids will float on water.
- Substance may be transported hot.
- For hybrid vehicles, GUIDE 147 (lithium ion batteries) or GUIDE 138 (sodium batteries) should also be consulted.
- **If molten aluminum is involved, refer to GUIDE 169.**

HEALTH

CAUTION: Petroleum crude oil (UN1267) may contain **TOXIC** hydrogen sulphide gas.

- Inhalation or contact with material may irritate or burn skin and eyes.
- Fire may produce irritating, corrosive and/or toxic gases.
- Vapors may cause dizziness or asphyxiation.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 50 meters (150 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 300 meters (1000 feet).

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

CAUTION: The majority of these products have a very low flash point. Use of water spray when fighting fire may be inefficient.

CAUTION: For mixtures containing alcohol or polar solvent, alcohol-resistant foam may be more effective.

Small Fire

- Dry chemical, CO_2, water spray or regular foam.

Large Fire

- Water spray, fog or regular foam.
- Avoid aiming straight or solid streams directly onto the product.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- For petroleum crude oil, do not spray water directly into a breached tank car. This can lead to a dangerous boil over.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- Prevent entry into waterways, sewers, basements or confined areas.
- A vapor-suppressing foam may be used to reduce vapors.
- Absorb or cover with dry earth, sand or other non-combustible material and transfer to containers.
- Use clean, non-sparking tools to collect absorbed material.

Large Spill

- Dike far ahead of liquid spill for later disposal.
- Water spray may reduce vapor, but may not prevent ignition in closed spaces.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Wash skin with soap and water.
- In case of burns, immediately cool affected skin for as long as possible with cold water. Do not remove clothing if adhering to skin.
- Keep victim calm and warm.

GUIDE 129 Flammable Liquids (Water-Miscible/Noxious)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- **HIGHLY FLAMMABLE: Will be easily ignited by heat, sparks or flames.**
- Vapors may form explosive mixtures with air.
- Vapors may travel to source of ignition and flash back.
- Most vapors are heavier than air. They will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Vapor explosion hazard indoors, outdoors or in sewers.
- Those substances designated with a **(P)** may polymerize explosively when heated or involved in a fire.
- Runoff to sewer may create fire or explosion hazard.
- Containers may explode when heated.
- Many liquids will float on water.

HEALTH

- May cause toxic effects if inhaled or absorbed through skin.
- Inhalation or contact with material may irritate or burn skin and eyes.
- Fire will produce irritating, corrosive and/or toxic gases.
- Vapors may cause dizziness or asphyxiation.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection.**

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 50 meters (150 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 300 meters (1000 feet).

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

CAUTION: The majority of these products have a very low flash point. Use of water spray when fighting fire may be inefficient.

Small Fire

- Dry chemical, CO_2, water spray or alcohol-resistant foam.
- **Do not use dry chemical extinguishers to control fires involving nitromethane (UN1261) or nitroethane (UN2842).**

Large Fire

- Water spray, fog or alcohol-resistant foam.
- Avoid aiming straight or solid streams directly onto the product.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- Prevent entry into waterways, sewers, basements or confined areas.
- A vapor-suppressing foam may be used to reduce vapors.
- Absorb or cover with dry earth, sand or other non-combustible material and transfer to containers.
- Use clean, non-sparking tools to collect absorbed material.

Large Spill

- Dike far ahead of liquid spill for later disposal.
- Water spray may reduce vapor, but may not prevent ignition in closed spaces.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Wash skin with soap and water.
- In case of burns, immediately cool affected skin for as long as possible with cold water. Do not remove clothing if adhering to skin.
- Keep victim calm and warm.
- Effects of exposure (inhalation, ingestion or skin contact) to substance may be delayed.

GUIDE 130 Flammable Liquids (Water-Immiscible/Noxious)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- **HIGHLY FLAMMABLE: Will be easily ignited by heat, sparks or flames.**
- Vapors may form explosive mixtures with air.
- Vapors may travel to source of ignition and flash back.
- Most vapors are heavier than air. They will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Vapor explosion hazard indoors, outdoors or in sewers.
- Those substances designated with a **(P)** may polymerize explosively when heated or involved in a fire.
- Runoff to sewer may create fire or explosion hazard.
- Containers may explode when heated.
- Many liquids will float on water.

HEALTH

- May cause toxic effects if inhaled or absorbed through skin.
- Inhalation or contact with material may irritate or burn skin and eyes.
- Fire will produce irritating, corrosive and/or toxic gases.
- Vapors may cause dizziness or asphyxiation.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 50 meters (150 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 300 meters (1000 feet).

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

EMERGENCY RESPONSE

FIRE

CAUTION: The majority of these products have a very low flash point. Use of water spray when fighting fire may be inefficient.

Small Fire

- Dry chemical, CO_2, water spray or regular foam.

Large Fire

- Water spray, fog or regular foam.
- Avoid aiming straight or solid streams directly onto the product.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- Prevent entry into waterways, sewers, basements or confined areas.
- A vapor-suppressing foam may be used to reduce vapors.
- Absorb or cover with dry earth, sand or other non-combustible material and transfer to containers.
- Use clean, non-sparking tools to collect absorbed material.

Large Spill

- Dike far ahead of liquid spill for later disposal.
- Water spray may reduce vapor, but may not prevent ignition in closed spaces.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Wash skin with soap and water.
- In case of burns, immediately cool affected skin for as long as possible with cold water. Do not remove clothing if adhering to skin.
- Keep victim calm and warm.
- Effects of exposure (inhalation, ingestion or skin contact) to substance may be delayed.

POTENTIAL HAZARDS

HEALTH

- **TOXIC; may be fatal if inhaled, ingested or absorbed through skin.**
- Inhalation or contact with some of these materials will irritate or burn skin and eyes.
- Fire will produce irritating, corrosive and/or toxic gases.
- Vapors may cause dizziness or asphyxiation.
- Runoff from fire control or dilution water may cause environmental contamination.

FIRE OR EXPLOSION

- **HIGHLY FLAMMABLE: Will be easily ignited by heat, sparks or flames.**

CAUTION: Methanol (UN1230) will burn with an invisible flame. Use an alternate method of detection (thermal camera, broom handle, etc.)

- Vapors may form explosive mixtures with air.
- Vapors may travel to source of ignition and flash back.
- Most vapors are heavier than air. They will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Vapor explosion and poison hazard indoors, outdoors or in sewers.
- Those substances designated with a **(P)** may polymerize explosively when heated or involved in a fire.
- Runoff to sewer may create fire or explosion hazard.
- Containers may explode when heated.
- Many liquids will float on water.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 50 meters (150 feet) in all directions.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

CAUTION: The majority of these products have a very low flash point. Use of water spray when fighting fire may be inefficient.

CAUTION: Methanol (UN1230) will burn with an invisible flame. Use an alternate method of detection (thermal camera, broom handle, etc.)

Small Fire

- Dry chemical, CO_2, water spray or alcohol-resistant foam.

Large Fire

- Water spray, fog or alcohol-resistant foam.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Dike runoff from fire control for later disposal.
- Avoid aiming straight or solid streams directly onto the product.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- Prevent entry into waterways, sewers, basements or confined areas.
- A vapor-suppressing foam may be used to reduce vapors.

Small Spill

- Absorb with earth, sand or other non-combustible material and transfer to containers for later disposal.
- Use clean, non-sparking tools to collect absorbed material.

Large Spill

- Dike far ahead of liquid spill for later disposal.
- Water spray may reduce vapor, but may not prevent ignition in closed spaces.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves. • Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Wash skin with soap and water.
- In case of burns, immediately cool affected skin for as long as possible with cold water. Do not remove clothing if adhering to skin. • Keep victim calm and warm.
- Effects of exposure (inhalation, ingestion or skin contact) to substance may be delayed.

GUIDE 132 Flammable Liquids - Corrosive

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- Flammable/combustible material.
- May be ignited by heat, sparks or flames.
- Vapors may form explosive mixtures with air.
- Vapors may travel to source of ignition and flash back.
- Most vapors are heavier than air. They will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Vapor explosion hazard indoors, outdoors or in sewers.
- Those substances designated with a **(P)** may polymerize explosively when heated or involved in a fire.
- Runoff to sewer may create fire or explosion hazard.
- Containers may explode when heated.
- Many liquids will float on water.

HEALTH

- May cause toxic effects if inhaled or ingested.
- Contact with substance may cause severe burns to skin and eyes.
- Fire will produce irritating, corrosive and/or toxic gases.
- Vapors may cause dizziness or asphyxiation.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 50 meters (150 feet) in all directions.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- **Some of these materials may react violently with water.**

Small Fire

- Dry chemical, CO_2, water spray or alcohol-resistant foam.

Large Fire

- Water spray, fog or alcohol-resistant foam.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Dike runoff from fire control for later disposal.
- Do not get water inside containers.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- Prevent entry into waterways, sewers, basements or confined areas.
- A vapor-suppressing foam may be used to reduce vapors.
- Absorb with earth, sand or other non-combustible material.
- For **hydrazine**, absorb with DRY sand or inert absorbent (vermiculite or absorbent pads).
- Use clean, non-sparking tools to collect absorbed material.

Large Spill

- Dike far ahead of liquid spill for later disposal.
- Water spray may reduce vapor, but may not prevent ignition in closed spaces.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- In case of burns, immediately cool affected skin for as long as possible with cold water. Do not remove clothing if adhering to skin.
- Keep victim calm and warm.
- Effects of exposure (inhalation, ingestion or skin contact) to substance may be delayed.

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- Flammable/combustible material.
- May be ignited by friction, heat, sparks or flames.
- Some may burn rapidly with flare-burning effect.
- Powders, dusts, shavings, borings, turnings or cuttings may explode or burn with explosive violence.
- Substance may be transported in a molten form at a temperature that may be above its flash point.
- May re-ignite after fire is extinguished.

HEALTH

- Fire may produce irritating and/or toxic gases.
- Contact may cause burns to skin and eyes.
- Contact with molten substance may cause severe burns to skin and eyes.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 25 meters (75 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 100 meters (330 feet).

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

- Dry chemical, CO_2, sand, earth, water spray or regular foam.

Large Fire

- Water spray, fog or regular foam.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Metal Pigments or Pastes (e.g. "Aluminum Paste")

- Aluminum Paste fires should be treated as a combustible metal fire. Use DRY sand, graphite powder, dry sodium chloride-based extinguishers or class D extinguishers. Also, see GUIDE 170.

Fire Involving Tanks or Car/Trailer Loads

- Cool containers with flooding quantities of water until well after fire is out.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Do not touch or walk through spilled material.

Small Dry Spill

- With clean shovel, place material into clean, dry container and cover loosely; move containers from spill area.

Large Spill

- Wet down with water and dike for later disposal.
- Prevent entry into waterways, sewers, basements or confined areas.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Removal of solidified molten material from skin requires medical assistance.
- Keep victim calm and warm.

GUIDE 134 Flammable Solids - Toxic and/or Corrosive

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- Flammable/combustible material.
- May be ignited by heat, sparks or flames.
- When heated, vapors may form explosive mixtures with air: indoors, outdoors and sewers explosion hazards.
- Contact with metals may evolve flammable hydrogen gas.
- Containers may explode when heated.

HEALTH

- **TOXIC;** inhalation, ingestion or skin contact with material may cause severe injury or death.
- Fire will produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may be corrosive and/or toxic and cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper**. If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Stay upwind, uphill and/or upstream.
- Keep unauthorized personnel away.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 25 meters (75 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 100 meters (330 feet).

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

- Dry chemical, CO_2, water spray or alcohol-resistant foam.

Large Fire

- Water spray, fog or alcohol-resistant foam.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Avoid aiming straight or solid streams directly onto the product.
- Do not get water inside containers.
- Dike runoff from fire control for later disposal.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Stop leak if you can do it without risk.
- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Prevent entry into waterways, sewers, basements or confined areas.
- Use clean, non-sparking tools to collect material and place it into loosely covered plastic containers for later disposal.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- For minor skin contact, avoid spreading material on unaffected skin.
- Keep victim calm and warm.
- Effects of exposure (inhalation, ingestion or skin contact) to substance may be delayed.

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- Flammable/combustible material.
- May ignite on contact with moist air or moisture.
- May burn rapidly with flare-burning effect.
- Some react vigorously or explosively on contact with water.
- Some may decompose explosively when heated or involved in a fire.
- May re-ignite after fire is extinguished.
- Runoff may create fire or explosion hazard.
- Containers may explode when heated.

HEALTH

- Fire will produce irritating, corrosive and/or toxic gases.
- Inhalation of decomposition products may cause severe injury or death.
- Contact with substance may cause severe burns to skin and eyes.
- Runoff from fire control or dilution water may cause environmental contamination.

CAUTION: Pentaborane (UN1380) is highly toxic and may be fatal if inhaled, ingested or absorbed through skin.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Stay upwind, uphill and/or upstream.
- Keep unauthorized personnel away.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- **DO NOT USE WATER, CO_2 OR FOAM ON MATERIAL ITSELF.**
- Some of these materials may react violently with water.

CAUTION: For Xanthates, UN3342 and for Dithionite (Hydrosulfite/Hydrosulphite) UN1384, UN1923 and UN1929, USE FLOODING AMOUNTS OF WATER for SMALL AND LARGE fires to stop the reaction. Smothering will not work for these materials, they do not need air to burn.

Small Fire

- Dry chemical, soda ash, lime or DRY sand, **EXCEPT for UN1384, UN1923, UN1929 and UN3342**.

Large Fire

- DRY sand, dry chemical, soda ash or lime **EXCEPT for UN1384, UN1923, UN1929 and UN3342**, or withdraw from area and let fire burn.

CAUTION: UN3342 when flooded with water will continue to evolve flammable Carbon disulfide/Carbon disulphide vapors.

- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Do not get water inside containers or in contact with substance.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.

Small Spill

CAUTION: For spills of Xanthates, UN3342 and for Dithionite (Hydrosulfite/Hydrosulphite), UN1384, UN1923 and UN1929, dissolve in 5 parts water and collect for proper disposal.

CAUTION: UN3342 when flooded with water will continue to evolve flammable Carbon disulfide/Carbon disulphide vapors.

- Cover with DRY earth, DRY sand or other non-combustible material followed with plastic sheet to minimize spreading or contact with rain.
- Use clean, non-sparking tools to collect material and place it into loosely covered plastic containers for later disposal.
- Prevent entry into waterways, sewers, basements or confined areas.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.

GUIDE 136 Substances - Spontaneously Combustible - Toxic and/or Corrosive (Air-Reactive)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- Extremely flammable; will ignite itself if exposed to air.
- Burns rapidly, releasing dense, white, irritating fumes.
- Substance may be transported in a molten form.
- May re-ignite after fire is extinguished.
- Corrosive substances in contact with metals may produce flammable hydrogen gas.
- Containers may explode when heated.

HEALTH

- Fire will produce irritating, corrosive and/or toxic gases.
- **TOXIC**; ingestion of substance or inhalation of decomposition products will cause severe injury or death.
- Contact with substance may cause severe burns to skin and eyes.
- Some effects may be experienced due to skin absorption.
- Runoff from fire control or dilution water may be corrosive and/or toxic and cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Stay upwind, uphill and/or upstream.
- Keep unauthorized personnel away.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.
- **For Phosphorus (UN1381): Special aluminized protective clothing should be worn when direct contact with the substance is possible.**

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Spill

- Consider initial downwind evacuation for at least 300 meters (1000 feet).

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

- Water spray, wet sand or wet earth.

Large Fire

- Water spray or fog.
- **Do not scatter spilled material with high-pressure water streams.**
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Do not touch or walk through spilled material.
- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Stop leak if you can do it without risk.

Small Spill

- Cover with water, sand or earth. Shovel into metal container and keep material under water.

Large Spill

- Dike for later disposal and cover with wet sand or earth.
- Prevent entry into waterways, sewers, basements or confined areas.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- In case of contact with substance, keep exposed skin areas immersed in water or covered with wet bandages until medical attention is received.
- Removal of solidified molten material from skin requires medical assistance.
- Remove and isolate contaminated clothing and shoes at the site and place in metal container filled with water. Fire hazard if allowed to dry.
- Effects of exposure (inhalation, ingestion or skin contact) to substance may be delayed.
- Keep victim calm and warm.

POTENTIAL HAZARDS

HEALTH

- CORROSIVE and/or TOXIC; inhalation, ingestion or contact (skin, eyes) with vapors, dusts or substance may cause severe injury, burns or death.
- Fire will produce irritating, corrosive and/or toxic gases.
- Reaction with water may generate much heat that will increase the concentration of fumes in the air.
- Contact with molten substance may cause severe burns to skin and eyes.
- Runoff from fire control or dilution water may cause environmental contamination.

FIRE OR EXPLOSION

- **EXCEPT FOR ACETIC ANHYDRIDE (UN1715), THAT IS FLAMMABLE,** some of these materials may burn, but none ignite readily.
- May ignite combustibles (wood, paper, oil, clothing, etc.).
- Substance will react with water (some violently), releasing corrosive and/or toxic gases and runoff.
- Flammable/toxic gases may accumulate in confined areas (basement, tanks, hopper/tank cars, etc.).
- Contact with metals may evolve flammable hydrogen gas.
- Containers may explode when heated or if contaminated with water.
- Substance may be transported in a molten form.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- **When material is not involved in fire, do not use water on material itself.**

Small Fire

- Dry chemical or CO_2.
- If it can be done safely, move undamaged containers away from the area around the fire.

Large Fire

- Flood fire area with large quantities of water, while knocking down vapors with water fog. If insufficient water supply, responders should withdraw.

Fire Involving Tanks or Car/Trailer Loads

- Cool containers with flooding quantities of water until well after fire is out.
- Do not get water inside containers.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Stop leak if you can do it without risk.
- Use water spray to reduce vapors; do not put water directly on leak, spill area or inside container.
- Keep combustibles (wood, paper, oil, etc.) away from spilled material.

Small Spill

- Cover with DRY earth, DRY sand or other non-combustible material followed with plastic sheet to minimize spreading or contact with rain.
- Use clean, non-sparking tools to collect material and place it into loosely covered plastic containers for later disposal.
- Prevent entry into waterways, sewers, basements or confined areas.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- For minor skin contact, avoid spreading material on unaffected skin.
- Removal of solidified molten material from skin requires medical assistance.
- Keep victim calm and warm.
- Effects of exposure (inhalation, ingestion or skin contact) to substance may be delayed.

GUIDE 138 Substances - Water-Reactive (Emitting Flammable Gases)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- Produce flammable gases on contact with water.
- May ignite on contact with water or moist air.
- Some react vigorously or explosively on contact with water.
- May be ignited by heat, sparks or flames.
- May re-ignite after fire is extinguished.
- Some are transported in highly flammable liquids.
- Runoff may create fire or explosion hazard.

HEALTH

- Inhalation or contact with vapors, substance or decomposition products may cause severe injury or death.
- May produce corrosive solutions on contact with water.
- Fire will produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- **DO NOT USE WATER OR FOAM.**

Small Fire

- Dry chemical, soda ash, lime or sand.

Large Fire

- DRY sand, dry chemical, soda ash or lime or withdraw from area and let fire burn.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Metals or Powders (Aluminum, Lithium, Magnesium, etc.)

- Use dry chemical, DRY sand, sodium chloride powder, graphite powder or class D extinguishers; in addition, for Lithium you may use Lith-X® powder or copper powder. Also, see GUIDE 170.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Do not get water inside containers.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- **DO NOT GET WATER on spilled substance or inside containers.**

Small Spill

- Cover with DRY earth, DRY sand or other non-combustible material followed with plastic sheet to minimize spreading or contact with rain.
- Dike for later disposal; do not apply water unless directed to do so.

Powder Spill

- Cover powder spill with plastic sheet or tarp to minimize spreading and keep powder dry.
- **DO NOT CLEAN-UP OR DISPOSE OF, EXCEPT UNDER SUPERVISION OF A SPECIALIST.**

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, wipe from skin immediately; flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.

GUIDE 139 Substances - Water-Reactive (Emitting Flammable And Toxic Gases)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- Produce flammable and toxic gases on contact with water.
- May ignite on contact with water or moist air.
- Some react vigorously or explosively on contact with water.
- May be ignited by heat, sparks or flames.
- May re-ignite after fire is extinguished.
- Some are transported in highly flammable liquids.
- Containers may explode when heated.
- Runoff may create fire or explosion hazard.

HEALTH

- Highly toxic: contact with water produces toxic gas, may be fatal if inhaled.
- Inhalation or contact with vapors, substance or decomposition products may cause severe injury or death.
- May produce corrosive solutions on contact with water.
- Fire will produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- **DO NOT USE WATER OR FOAM. (FOAM MAY BE USED FOR CHLOROSILANES, SEE BELOW)**

Small Fire

- Dry chemical, soda ash, lime or sand.

Large Fire

- DRY sand, dry chemical, soda ash or lime or withdraw from area and let fire burn.
- **FOR CHLOROSILANES, DO NOT USE WATER**; use AFFF alcohol-resistant medium-expansion foam; **DO NOT USE** dry chemicals, soda ash or lime on chlorosilane fires (large or small) as they may release large quantities of hydrogen gas that may explode.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Do not get water inside containers.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- **DO NOT GET WATER on spilled substance or inside containers.**
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- **FOR CHLOROSILANES**, use AFFF alcohol-resistant medium-expansion foam to reduce vapors.

Small Spill

- Cover with DRY earth, DRY sand or other non-combustible material followed with plastic sheet to minimize spreading or contact with rain.
- Dike for later disposal; do not apply water unless directed to do so.

Powder Spill

- Cover powder spill with plastic sheet or tarp to minimize spreading and keep powder dry.
- **DO NOT CLEAN-UP OR DISPOSE OF, EXCEPT UNDER SUPERVISION OF A SPECIALIST.**

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, wipe from skin immediately; flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- These substances will accelerate burning when involved in a fire.
- Some may decompose explosively when heated or involved in a fire.
- May explode from heat or contamination.
- Some will react explosively with hydrocarbons (fuels).
- May ignite combustibles (wood, paper, oil, clothing, etc.).
- Containers may explode when heated.
- Runoff may create fire or explosion hazard.

HEALTH

- Inhalation, ingestion or contact (skin, eyes) with vapors or substance may cause severe injury, burns or death.
- Fire may produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Large Spill

- Consider initial downwind evacuation for at least 100 meters (330 feet).

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.
- If **ammonium nitrate** is in a tank, rail car or tank truck and involved in a fire, ISOLATE for 1600 meters (1 mile) in all directions; also, initiate evacuation including emergency responders for 1600 meters (1 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

- Use water. Do not use dry chemicals or foams. CO_2 or Halon® may provide limited control.

Large Fire

- Flood fire area with water from a distance.
- Do not move cargo or vehicle if cargo has been exposed to heat.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- Keep combustibles (wood, paper, oil, etc.) away from spilled material.
- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Stop leak if you can do it without risk.
- Do not get water inside containers.

Small Dry Spill

- With clean shovel, place material into clean, dry container and cover loosely; move containers from spill area.

Small Liquid Spill

- Use a non-combustible material like vermiculite or sand to soak up the product and place into a container for later disposal.

Large Spill

- Dike far ahead of liquid spill for later disposal.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- Contaminated clothing may be a fire risk when dry.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- These substances will accelerate burning when involved in a fire.
- May explode from heat or contamination.
- Some may burn rapidly.
- Some will react explosively with hydrocarbons (fuels).
- May ignite combustibles (wood, paper, oil, clothing, etc.).
- Containers may explode when heated.
- Runoff may create fire or explosion hazard.

HEALTH

- Toxic by ingestion.
- Inhalation of dust is toxic.
- Fire may produce irritating, corrosive and/or toxic gases.
- Contact with substance may cause severe burns to skin and eyes.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper**. If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Large Spill

- Consider initial downwind evacuation for at least 100 meters (330 feet).

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

- Use water. Do not use dry chemicals or foams. CO_2 or Halon® may provide limited control.

Large Fire

- Flood fire area with water from a distance.
- Do not move cargo or vehicle if cargo has been exposed to heat.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- Keep combustibles (wood, paper, oil, etc.) away from spilled material.
- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Stop leak if you can do it without risk.

Small Dry Spill

- With clean shovel, place material into clean, dry container and cover loosely; move containers from spill area.

Large Spill

- Dike far ahead of spill for later disposal.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- Contaminated clothing may be a fire risk when dry.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.

GUIDE 142 Oxidizers - Toxic (Liquid)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- These substances will accelerate burning when involved in a fire.
- May explode from heat or contamination.
- Some will react explosively with hydrocarbons (fuels).
- May ignite combustibles (wood, paper, oil, clothing, etc.).
- Containers may explode when heated.
- Runoff may create fire or explosion hazard.

HEALTH

- **TOXIC;** inhalation, ingestion or contact (skin, eyes) with vapors or substance may cause severe injury, burns or death.
- Fire may produce irritating, corrosive and/or toxic gases.
- Toxic/flammable fumes may accumulate in confined areas (basement, tanks, tank cars, etc.).
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 50 meters (150 feet) in all directions.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

- Use water. Do not use dry chemicals or foams. CO_2 or Halon® may provide limited control.

Large Fire

- Flood fire area with water from a distance.
- Do not move cargo or vehicle if cargo has been exposed to heat.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- Keep combustibles (wood, paper, oil, etc.) away from spilled material.
- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Stop leak if you can do it without risk.
- Use water spray to reduce vapors or divert vapor cloud drift.
- Do not get water inside containers.

Small Liquid Spill

- Use a non-combustible material like vermiculite or sand to soak up the product and place into a container for later disposal.

Large Spill

- Dike far ahead of liquid spill for later disposal.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- Contaminated clothing may be a fire risk when dry.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.

GUIDE 143 Oxidizers (Unstable)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- May explode from friction, heat or contamination.
- These substances will accelerate burning when involved in a fire.
- May ignite combustibles (wood, paper, oil, clothing, etc.).
- Some will react explosively with hydrocarbons (fuels).
- Containers may explode when heated.
- Runoff may create fire or explosion hazard.

HEALTH

- **TOXIC;** inhalation, ingestion or contact (skin, eyes) with vapors, dusts or substance may cause severe injury, burns or death.
- Fire may produce irritating and/or toxic gases.
- Toxic fumes or dust may accumulate in confined areas (basement, tanks, hopper/tank cars, etc.).
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

- Use water. Do not use dry chemicals or foams. CO_2 or Halon® may provide limited control.

Large Fire

- Flood fire area with water from a distance.
- Do not move cargo or vehicle if cargo has been exposed to heat.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Do not get water inside containers: a violent reaction may occur.

Fire Involving Tanks or Car/Trailer Loads

- Cool containers with flooding quantities of water until well after fire is out.
- Dike runoff from fire control for later disposal.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- Keep combustibles (wood, paper, oil, etc.) away from spilled material.
- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Use water spray to reduce vapors or divert vapor cloud drift.
- Prevent entry into waterways, sewers, basements or confined areas.

Small Spill

- Flush area with large amounts of water.

Large Spill

- **DO NOT CLEAN-UP OR DISPOSE OF, EXCEPT UNDER SUPERVISION OF A SPECIALIST.**

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- Contaminated clothing may be a fire risk when dry.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.

GUIDE 144 Oxidizers (Water-Reactive)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- May ignite combustibles (wood, paper, oil, clothing, etc.).
- React vigorously and/or explosively with water.
- Produce toxic and/or corrosive substances on contact with water.
- Flammable/toxic gases may accumulate in tanks and hopper cars.
- Some may produce flammable hydrogen gas upon contact with metals.
- Containers may explode when heated.
- Runoff may create fire or explosion hazard.

HEALTH

- **TOXIC;** inhalation or contact with vapor, substance, or decomposition products may cause severe injury or death.
- Fire will produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- **DO NOT USE WATER OR FOAM.**

Small Fire

- Dry chemical, soda ash or lime.

Large Fire

- DRY sand, dry chemical, soda ash or lime or withdraw from area and let fire burn.
- Do not move cargo or vehicle if cargo has been exposed to heat.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Stop leak if you can do it without risk.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- **DO NOT GET WATER on spilled substance or inside containers.**

Small Spill

- Cover with DRY earth, DRY sand or other non-combustible material followed with plastic sheet to minimize spreading or contact with rain.

Large Spill

- **DO NOT CLEAN-UP OR DISPOSE OF, EXCEPT UNDER SUPERVISION OF A SPECIALIST.**

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- Contaminated clothing may be a fire risk when dry.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.
- Keep victim under observation.
- Effects of contact or inhalation may be delayed.

GUIDE 145 Organic Peroxides (Heat and Contamination Sensitive)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- May explode from heat or contamination.
- May ignite combustibles (wood, paper, oil, clothing, etc.).
- May be ignited by heat, sparks or flames.
- May burn rapidly with flare-burning effect.
- Containers may explode when heated.
- Runoff may create fire or explosion hazard.

HEALTH

- Fire may produce irritating, corrosive and/or toxic gases.
- Ingestion or contact (skin, eyes) with substance may cause severe injury or burns.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Large Spill

- Consider initial evacuation for at least 250 meters (800 feet) in all directions.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

EMERGENCY RESPONSE

FIRE

Small Fire

- Water spray or fog is preferred; if water not available use dry chemical, CO_2 or regular foam.

Large Fire

- Flood fire area with water from a distance.
- Use water spray or fog; avoid aiming straight or solid streams directly onto the product.
- Do not move cargo or vehicle if cargo has been exposed to heat.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Keep combustibles (wood, paper, oil, etc.) away from spilled material.
- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Keep substance wet using water spray.
- Stop leak if you can do it without risk.

Small Spill

- Pick up with inert, damp, non-combustible material using clean, non-sparking tools and place into loosely covered plastic containers for later disposal.

Large Spill

- Wet down with water and dike for later disposal.
- Prevent entry into waterways, sewers, basements or confined areas.
- **DO NOT CLEAN-UP OR DISPOSE OF, EXCEPT UNDER SUPERVISION OF A SPECIALIST.**

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- Contaminated clothing may be a fire risk when dry.
- Remove material from skin immediately.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.

GUIDE 146 Organic Peroxides (Heat, Contamination and Friction Sensitive)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- May explode from heat, shock, friction or contamination.
- May ignite combustibles (wood, paper, oil, clothing, etc.).
- May be ignited by heat, sparks or flames.
- May burn rapidly with flare-burning effect.
- Containers may explode when heated.
- Runoff may create fire or explosion hazard.

HEALTH

- Fire may produce irritating, corrosive and/or toxic gases.
- Ingestion or contact (skin, eyes) with substance may cause severe injury or burns.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Large Spill

- Consider initial evacuation for at least 250 meters (800 feet) in all directions.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

- Water spray or fog is preferred; if water not available use dry chemical, CO_2 or regular foam.

Large Fire

- Flood fire area with water from a distance.
- Use water spray or fog; avoid aiming straight or solid streams directly onto the product.
- Do not move cargo or vehicle if cargo has been exposed to heat.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Keep combustibles (wood, paper, oil, etc.) away from spilled material.
- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Keep substance wet using water spray.
- Stop leak if you can do it without risk.

Small Spill

- Pick up with inert, damp, non-combustible material using clean, non-sparking tools and place into loosely covered plastic containers for later disposal.

Large Spill

- Wet down with water and dike for later disposal.
- Prevent entry into waterways, sewers, basements or confined areas.
- **DO NOT CLEAN-UP OR DISPOSE OF, EXCEPT UNDER SUPERVISION OF A SPECIALIST.**

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- Contaminated clothing may be a fire risk when dry.
- Remove material from skin immediately.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- Lithium ion batteries contain flammable liquid electrolyte that may vent, ignite and produce sparks when subjected to high temperatures (> 150°C (302°F)), when damaged or abused (e.g., mechanical damage or electrical overcharging).
- May burn rapidly with flare-burning effect.
- May ignite other batteries in close proximity.

HEALTH

- Contact with battery electrolyte may be irritating to skin, eyes and mucous membranes.
- Fire will produce irritating, corrosive and/or toxic gases.
- Burning batteries may produce toxic hydrogen fluoride gas (see GUIDE 125).
- Fumes may cause dizziness or asphyxiation.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 25 meters (75 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 100 meters (330 feet).

Fire

- If rail car or trailer is involved in a fire, ISOLATE for 500 meters (1/3 mile) in all directions; also initiate evacuation including emergency responders for 500 meters (1/3 mile) in all directions.

EMERGENCY RESPONSE

FIRE

Small Fire

- Dry chemical, CO_2, water spray or regular foam.

Large Fire

- Water spray, fog or regular foam.
- If it can be done safely, move undamaged containers away from the area around the fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Do not touch or walk through spilled material.
- Absorb with earth, sand or other non-combustible material.
- Leaking batteries and contaminated absorbent material should be placed in metal containers.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.

GUIDE 148 Organic Peroxides (Heat and Contamination Sensitive/Temperature Controlled)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- May explode from heat, contamination or loss of temperature control.
- These materials are particularly sensitive to temperature rises. Above a given "Control Temperature" they decompose violently and catch fire.
- May ignite combustibles (wood, paper, oil, clothing, etc.).
- May ignite spontaneously if exposed to air.
- May be ignited by heat, sparks or flames.
- May burn rapidly with flare-burning effect.
- Containers may explode when heated.
- Runoff may create fire or explosion hazard.

HEALTH

- Fire may produce irritating, corrosive and/or toxic gases.
- Ingestion or contact (skin, eyes) with substance may cause severe injury or burns.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Large Spill

- Consider initial evacuation for at least 250 meters (800 feet) in all directions.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- **The temperature of the substance must be maintained at or below the "Control Temperature" at all times.**

Small Fire

- Water spray or fog is preferred; if water not available use dry chemical, CO_2 or regular foam.

Large Fire

- Flood fire area with water from a distance.
- Use water spray or fog; avoid aiming straight or solid streams directly onto the product.
- Do not move cargo or vehicle if cargo has been exposed to heat.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- **BEWARE OF POSSIBLE CONTAINER EXPLOSION.**
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- **DO NOT allow the substance to warm up. Use a coolant agent such as dry ice or ice (wear thermal protective gloves). If this is not possible or none can be obtained, evacuate the area immediately.**
- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Keep combustibles (wood, paper, oil, etc.) away from spilled material.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.

Small Spill

- Pick up with inert, damp, non-combustible material using clean, non-sparking tools and place into loosely covered plastic containers for later disposal.

Large Spill

- Dike far ahead of liquid spill for later disposal.
- Prevent entry into waterways, sewers, basements or confined areas.
- **DO NOT CLEAN-UP OR DISPOSE OF, EXCEPT UNDER SUPERVISION OF A SPECIALIST.**

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- Contaminated clothing may be a fire risk when dry.
- Remove material from skin immediately.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.

GUIDE 149 Substances (Self-Reactive)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- **Self-decomposition, self-polymerization, or self-ignition may be triggered by heat, chemical reaction, friction or impact.**
- May be ignited by heat, sparks or flames.
- Some may decompose explosively when heated or involved in a fire.
- Those substances designated with a **(P)** may polymerize explosively when heated or involved in a fire.
- May burn violently. Decomposition or polymerization may be self-accelerating and produce large amounts of gases.
- Vapors or dust may form explosive mixtures with air.

HEALTH

- Inhalation or contact with vapors, substance or decomposition products may cause severe injury or death.
- May produce irritating, toxic and/or corrosive gases.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Large Spill

- Consider initial evacuation for at least 250 meters (800 feet) in all directions.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

- Dry chemical, CO_2, water spray or regular foam.

Large Fire

- Flood fire area with water from a distance.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks or Car/Trailer Loads

- **BEWARE OF POSSIBLE CONTAINER EXPLOSION.**
- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.

Small Spill

- Pick up with inert, damp, non-combustible material using clean, non-sparking tools and place into loosely covered plastic containers for later disposal.
- Prevent entry into waterways, sewers, basements or confined areas.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.

GUIDE 150 Substances (Self-Reactive/ Temperature Controlled)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- **Self-decomposition, self-polymerization, or self-ignition may be triggered by heat, chemical reaction, friction or impact.**
- Self-accelerating decomposition may occur if the specific control temperature is not maintained.
- These materials are particularly sensitive to temperature rises. Above a given "Control Temperature" they decompose or polymerize violently and may catch fire.
- May be ignited by heat, sparks or flames.
- Those substances designated with a **(P)** may polymerize explosively when heated or involved in a fire.
- Some may decompose explosively when heated or involved in a fire.
- May burn violently. Decomposition or polymerization may be self-accelerating and produce large amounts of gases.
- Vapors or dust may form explosive mixtures with air.

HEALTH

- Inhalation or contact with vapors, substance or decomposition products may cause severe injury or death.
- May produce irritating, toxic and/or corrosive gases.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Large Spill

- Consider initial evacuation for at least 250 meters (800 feet) in all directions.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- **The temperature of the substance must be maintained at or below the "Control Temperature" at all times.**

Small Fire

- Dry chemical, CO_2, water spray or regular foam.

Large Fire

- Flood fire area with water from a distance.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks or Car/Trailer Loads

- **BEWARE OF POSSIBLE CONTAINER EXPLOSION.**
- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- **DO NOT allow the substance to warm up. Use a coolant agent such as dry ice or ice (wear thermal protective gloves). If this is not possible or none can be obtained, evacuate the area immediately.**
- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.

Small Spill

- Pick up with inert, damp, non-combustible material using clean, non-sparking tools and place into loosely covered plastic containers for later disposal.
- Prevent entry into waterways, sewers, basements or confined areas.
- **DO NOT CLEAN-UP OR DISPOSE OF, EXCEPT UNDER SUPERVISION OF A SPECIALIST.**

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.

POTENTIAL HAZARDS

HEALTH

- **Highly toxic**, may be fatal if inhaled, ingested or absorbed through skin.
- Avoid any skin contact.
- Effects of contact or inhalation may be delayed.
- Fire may produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may be corrosive and/or toxic and cause environmental contamination.

FIRE OR EXPLOSION

- Non-combustible, substance itself does not burn but may decompose upon heating to produce corrosive and/or toxic fumes.
- Containers may explode when heated.
- Runoff may pollute waterways.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

- Dry chemical, CO_2 or water spray.

Large Fire

- Water spray, fog or regular foam.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Dike runoff from fire control for later disposal.
- Avoid aiming straight or solid streams directly onto the product.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Do not get water inside containers.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Stop leak if you can do it without risk.
- Prevent entry into waterways, sewers, basements or confined areas.
- Cover with plastic sheet to prevent spreading.
- Absorb or cover with dry earth, sand or other non-combustible material and transfer to containers.
- DO NOT GET WATER INSIDE CONTAINERS.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- For minor skin contact, avoid spreading material on unaffected skin.
- Keep victim calm and warm.
- Effects of exposure (inhalation, ingestion or skin contact) to substance may be delayed.

GUIDE 152 Substances - Toxic (Combustible)

POTENTIAL HAZARDS

HEALTH

- **Highly toxic,** may be fatal if inhaled, ingested or absorbed through skin.
- Contact with molten substance may cause severe burns to skin and eyes.
- Avoid any skin contact.
- Effects of contact or inhalation may be delayed.
- Fire may produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may be corrosive and/or toxic and cause environmental contamination.

FIRE OR EXPLOSION

- Combustible material: may burn but does not ignite readily.
- Containers may explode when heated.
- Runoff may pollute waterways.
- Substance may be transported in a molten form.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

- Dry chemical, CO_2 or water spray.

Large Fire

- Water spray, fog or regular foam.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Dike runoff from fire control for later disposal.
- Avoid aiming straight or solid streams directly onto the product.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Do not get water inside containers.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Stop leak if you can do it without risk.
- Prevent entry into waterways, sewers, basements or confined areas.
- Cover with plastic sheet to prevent spreading.
- Absorb or cover with dry earth, sand or other non-combustible material and transfer to containers.
- DO NOT GET WATER INSIDE CONTAINERS.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- For minor skin contact, avoid spreading material on unaffected skin.
- Keep victim calm and warm.
- Effects of exposure (inhalation, ingestion or skin contact) to substance may be delayed.

GUIDE 153 Substances - Toxic and/or Corrosive (Combustible)

POTENTIAL HAZARDS

HEALTH

- **TOXIC**; inhalation, ingestion or skin contact with material may cause severe injury or death.
- Contact with molten substance may cause severe burns to skin and eyes.
- Avoid any skin contact.
- Effects of contact or inhalation may be delayed.
- Fire may produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may be corrosive and/or toxic and cause environmental contamination.

FIRE OR EXPLOSION

- Combustible material: may burn but does not ignite readily.
- When heated, vapors may form explosive mixtures with air: indoors, outdoors and sewers explosion hazards.
- Those substances designated with a **(P)** may polymerize explosively when heated or involved in a fire.
- Contact with metals may evolve flammable hydrogen gas.
- Containers may explode when heated.
- Runoff may pollute waterways.
- Substance may be transported in a molten form.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

- Dry chemical, CO_2 or water spray.

Large Fire

- Dry chemical, CO_2, alcohol-resistant foam or water spray.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Dike runoff from fire control for later disposal.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Do not get water inside containers.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Stop leak if you can do it without risk.
- Prevent entry into waterways, sewers, basements or confined areas.
- Absorb or cover with dry earth, sand or other non-combustible material and transfer to containers.
- DO NOT GET WATER INSIDE CONTAINERS.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- For minor skin contact, avoid spreading material on unaffected skin.
- Keep victim calm and warm.
- Effects of exposure (inhalation, ingestion or skin contact) to substance may be delayed.

GUIDE 154 Substances - Toxic and/or Corrosive (Non-Combustible)

POTENTIAL HAZARDS

HEALTH

- **TOXIC**; inhalation, ingestion or skin contact with material may cause severe injury or death.
- Contact with molten substance may cause severe burns to skin and eyes.
- Avoid any skin contact.
- Effects of contact or inhalation may be delayed.
- Fire may produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may be corrosive and/or toxic and cause environmental contamination.

FIRE OR EXPLOSION

- Non-combustible, substance itself does not burn but may decompose upon heating to produce corrosive and/or toxic fumes.
- Some are oxidizers and may ignite combustibles (wood, paper, oil, clothing, etc.).
- Contact with metals may evolve flammable hydrogen gas.
- Containers may explode when heated.
- For electric vehicles or equipment, GUIDE 147 (lithium ion batteries) or GUIDE 138 (sodium batteries) should also be consulted.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

- Dry chemical, CO_2 or water spray.

Large Fire

- Dry chemical, CO_2, alcohol-resistant foam or water spray.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Dike runoff from fire control for later disposal.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Do not get water inside containers.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Stop leak if you can do it without risk.
- Prevent entry into waterways, sewers, basements or confined areas.
- Absorb or cover with dry earth, sand or other non-combustible material and transfer to containers.
- DO NOT GET WATER INSIDE CONTAINERS.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- For minor skin contact, avoid spreading material on unaffected skin.
- Keep victim calm and warm.
- Effects of exposure (inhalation, ingestion or skin contact) to substance may be delayed.

GUIDE 155 Substances - Toxic and/or Corrosive (Flammable/Water-Sensitive)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- **HIGHLY FLAMMABLE: Will be easily ignited by heat, sparks or flames.**
- Vapors form explosive mixtures with air: indoors, outdoors and sewers explosion hazards.
- Most vapors are heavier than air. They will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Vapors may travel to source of ignition and flash back.
- Those substances designated with a **(P)** may polymerize explosively when heated or involved in a fire.
- Substance will react with water (some violently) releasing flammable, toxic or corrosive gases and runoff.
- Contact with metals may evolve flammable hydrogen gas.
- Containers may explode when heated or if contaminated with water.

HEALTH

- **TOXIC**; inhalation, ingestion or contact (skin, eyes) with vapors, dusts or substance may cause severe injury, burns or death.
- **Bromoacetates and chloroacetates are extremely irritating/lachrymators (cause eye irritation and flow of tears).**
- Reaction with water or moist air will release toxic, corrosive or flammable gases.
- Reaction with water may generate much heat that will increase the concentration of fumes in the air.
- Fire will produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may be corrosive and/or toxic and cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- Note: Most foams will react with the material and release corrosive/toxic gases.

CAUTION: For Acetyl chloride (UN1717), use CO_2 or dry chemical only.

Small Fire

- CO_2, dry chemical, dry sand, alcohol-resistant foam.

Large Fire

- Water spray, fog or alcohol-resistant foam.
- **FOR CHLOROSILANES, DO NOT USE WATER**; use AFFF alcohol-resistant medium-expansion foam.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Avoid aiming straight or solid streams directly onto the product.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Do not get water inside containers.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Stop leak if you can do it without risk.
- A vapor-suppressing foam may be used to reduce vapors.
- **FOR CHLOROSILANES**, use AFFF alcohol-resistant medium-expansion foam to reduce vapors.
- **DO NOT GET WATER on spilled substance or inside containers.**
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- Prevent entry into waterways, sewers, basements or confined areas.

Small Spill

- Cover with DRY earth, DRY sand or other non-combustible material followed with plastic sheet to minimize spreading or contact with rain.
- Use clean, non-sparking tools to collect material and place it into loosely covered plastic containers for later disposal.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- For minor skin contact, avoid spreading material on unaffected skin.
- Keep victim calm and warm.
- Effects of exposure (inhalation, ingestion or skin contact) to substance may be delayed.

GUIDE 156 Substances - Toxic and/or Corrosive (Combustible/Water-Sensitive)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- Combustible material: may burn but does not ignite readily.
- Substance will react with water (some violently) releasing flammable, toxic or corrosive gases and runoff.
- When heated, vapors may form explosive mixtures with air: indoors, outdoors and sewers explosion hazards.
- Most vapors are heavier than air. They will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Vapors may travel to source of ignition and flash back.
- Contact with metals may evolve flammable hydrogen gas.
- Containers may explode when heated or if contaminated with water.

HEALTH

- **TOXIC;** inhalation, ingestion or contact (skin, eyes) with vapors, dusts or substance may cause severe injury, burns or death.
- Contact with molten substance may cause severe burns to skin and eyes.
- Reaction with water or moist air will release toxic, corrosive or flammable gases.
- Reaction with water may generate much heat that will increase the concentration of fumes in the air.
- Fire will produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may be corrosive and/or toxic and cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- Note: Most foams will react with the material and release corrosive/toxic gases.

Small Fire

- CO_2, dry chemical, dry sand, alcohol-resistant foam.

Large Fire

- Water spray, fog or alcohol-resistant foam.
- **FOR CHLOROSILANES, DO NOT USE WATER**; use AFFF alcohol-resistant medium-expansion foam.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Avoid aiming straight or solid streams directly onto the product.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Do not get water inside containers.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Stop leak if you can do it without risk.
- A vapor-suppressing foam may be used to reduce vapors.
- **FOR CHLOROSILANES**, use AFFF alcohol-resistant medium-expansion foam to reduce vapors.
- **DO NOT GET WATER on spilled substance or inside containers.**
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- Prevent entry into waterways, sewers, basements or confined areas.

Small Spill

- Cover with DRY earth, DRY sand or other non-combustible material followed with plastic sheet to minimize spreading or contact with rain.
- Use clean, non-sparking tools to collect material and place it into loosely covered plastic containers for later disposal.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- For minor skin contact, avoid spreading material on unaffected skin.
- Keep victim calm and warm.
- Effects of exposure (inhalation, ingestion or skin contact) to substance may be delayed.

GUIDE 157 Substances - Toxic and/or Corrosive (Non-Combustible/Water-Sensitive)

POTENTIAL HAZARDS

HEALTH

- **TOXIC**; inhalation, ingestion or contact (skin, eyes) with vapors, dusts or substance may cause severe injury, burns or death.
- Reaction with water or moist air may release toxic, corrosive or flammable gases.
- Reaction with water may generate much heat that will increase the concentration of fumes in the air.
- Fire will produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may be corrosive and/or toxic and cause environmental contamination.

FIRE OR EXPLOSION

- Non-combustible, substance itself does not burn but may decompose upon heating to produce corrosive and/or toxic fumes.
- UN1796, UN1802, UN1826, UN2032, UN3084, UN3085, and, at concentrations above 65%, UN2031 may act as oxidizers. Also consult GUIDE 140.
- Vapors may accumulate in confined areas (basement, tanks, hopper/tank cars, etc.).
- Substance may react with water (some violently), releasing corrosive and/or toxic gases and runoff.
- Contact with metals may evolve flammable hydrogen gas.
- Containers may explode when heated or if contaminated with water.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- Note: Some foams will react with the material and release corrosive/toxic gases.

Small Fire

- CO_2 (except for Cyanides), dry chemical, dry sand, alcohol-resistant foam.

Large Fire

- Water spray, fog or alcohol-resistant foam.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Avoid aiming straight or solid streams directly onto the product.
- Dike runoff from fire control for later disposal.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Do not get water inside containers.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Stop leak if you can do it without risk.
- A vapor-suppressing foam may be used to reduce vapors.
- DO NOT GET WATER INSIDE CONTAINERS.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- Prevent entry into waterways, sewers, basements or confined areas.

Small Spill

- Cover with DRY earth, DRY sand or other non-combustible material followed with plastic sheet to minimize spreading or contact with rain.
- Use clean, non-sparking tools to collect material and place it into loosely covered plastic containers for later disposal.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- **In case of skin contact with Hydrofluoric acid (UN1790)**, if calcium gluconate gel is available, rinse 5 minutes, then apply gel. Otherwise, continue rinsing until medical treatment is available.
- For minor skin contact, avoid spreading material on unaffected skin.
- Keep victim calm and warm.
- Effects of exposure (inhalation, ingestion or skin contact) to substance may be delayed.

POTENTIAL HAZARDS

HEALTH

- Inhalation or contact with substance may cause infection, disease or death.
- Category A Infectious Substances (UN2814, UN2900 or UN3549) are more hazardous, or are in a more hazardous form, than infectious substances shipped as Category B Biological Substances (UN3373) or clinical waste/medical waste (UN3291).
- Runoff from fire control or dilution water may cause environmental contamination.
- Damaged packages containing solid CO_2 as a refrigerant may produce water or frost from condensation of air. Do not touch this liquid as it could be contaminated by the contents of the parcel.
- Contact with solid CO_2 may cause burns, severe injury and/or frostbite.

FIRE OR EXPLOSION

- Some of these materials may burn, but none ignite readily.
- Some may be transported in flammable liquids.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Consult the shipping paper to identify the substance involved.

PROTECTIVE CLOTHING

- Use judgement based on the amount of material present and the possible routes of exposure to select protective clothing.
- Wear appropriate respiratory protection, such as fit-tested N95 respirator (at minimum), powered air purifying respirator (PAPR), or positive pressure self-contained breathing apparatus (SCBA).
- Wear full coverage body protection (e.g., Tyvek suit), faceshield, and disposable fluid-resistant gloves (e.g., latex or nitrile).
- Wear appropriate footwear; disposable shoe covers can be worn to protect against contamination.
- Puncture- and cut-resistant gloves should be worn over fluid-resistant gloves if sharp objects (e.g., broken glass, needles) are present.
- Wear insulated gloves (e.g. cryo gloves) over fluid-resistant gloves when handling dry ice (UN1845).
- Decontaminate protective clothing and personal protective equipment after use and before cleaning or disposal with a compatible chemical disinfectant (e.g., 10% solution of bleach, equivalent to 0.5% sodium hypochlorite) or through a validated decontamination technology (e.g., autoclave) or process.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.
- For more information on decontamination, consult p. 362

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 25 meters (75 feet) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

- Dry chemical, soda ash, lime or sand.

Large Fire

- Use extinguishing agent suitable for type of surrounding fire.
- Do not scatter spilled material with high-pressure water streams.
- If it can be done safely, move undamaged containers away from the area around the fire.

SPILL OR LEAK

- Do not touch or walk through spilled material.
- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Absorb with earth, sand or other non-combustible material.
- Cover damaged package or spilled material with absorbent material such as paper towel, towel or rag to absorb any liquids, and, beginning from outside edge, pour liquid bleach or other chemical disinfectant to saturate. Keep wet with liquid bleach or other disinfectant.
- **DO NOT CLEAN-UP OR DISPOSE OF, EXCEPT UNDER SUPERVISION OF A SPECIALIST.**

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to a safe isolated area if it can be done safely.

CAUTION: Victim may be a source of contamination.

- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush eyes with running water and wash skin with soap and water for at least 20 minutes. Take caution not to break the skin.
- Effects of exposure (inhalation, ingestion, injection/inoculation or skin contact) to substance may be delayed. Victim should consult medical professional for information regarding symptoms and treatment.
- **For further assistance, contact your local Poison Control Center.**

GUIDE 159 Substances (Irritating)

POTENTIAL HAZARDS

HEALTH

- Inhalation of vapors or dust is extremely irritating.
- May cause burning of eyes and lachrymation (flow of tears).
- May cause coughing, difficult breathing and nausea.
- Brief exposure effects last only a few minutes.
- Exposure in an enclosed area may be very harmful.
- Fire will produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may cause environmental contamination.

FIRE OR EXPLOSION

- Some of these materials may burn, but none ignite readily.
- Containers may explode when heated.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

Small Fire

- Dry chemical, CO_2, water spray or regular foam.

Large Fire

- Water spray, fog or regular foam.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Dike runoff from fire control for later disposal.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Do not get water inside containers.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.

Small Spill

- Pick up with sand or other non-combustible absorbent material and place into containers for later disposal.

Large Spill

- Dike far ahead of liquid spill for later disposal.
- Prevent entry into waterways, sewers, basements or confined areas.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- For minor skin contact, avoid spreading material on unaffected skin.
- Keep victim calm and warm.
- Effects should disappear after individual has been exposed to fresh air for approximately 10 minutes.

POTENTIAL HAZARDS

HEALTH

- Toxic by ingestion.
- Vapors may cause dizziness or asphyxiation.
- Exposure in an enclosed area may be very harmful.
- Contact may irritate or burn skin and eyes.
- Fire may produce irritating and/or toxic gases.
- Runoff from fire control or dilution water may cause environmental contamination.

FIRE OR EXPLOSION

- Some of these materials may burn, but none ignite readily.
- Most vapors are heavier than air.
- Air/vapor mixtures may explode when ignited.
- Container may explode in heat of fire.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Many gases are heavier than air and will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 50 meters (150 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 100 meters (330 feet).

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

EMERGENCY RESPONSE

FIRE

Small Fire

- Dry chemical, CO_2 or water spray.

Large Fire

- Dry chemical, CO_2, alcohol-resistant foam or water spray.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Dike runoff from fire control for later disposal.

Fire Involving Tanks or Car/Trailer Loads

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Stop leak if you can do it without risk.

Small Liquid Spill

- Pick up with sand, earth or other non-combustible absorbent material.

Large Spill

- Dike far ahead of liquid spill for later disposal.
- Prevent entry into waterways, sewers, basements or confined areas.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- For minor skin contact, avoid spreading material on unaffected skin.
- Wash skin with soap and water.
- Keep victim calm and warm.

GUIDE 161 Radioactive Materials (Low Level Radiation)

POTENTIAL HAZARDS

HEALTH

- Radiation presents minimal risk to transport workers, emergency response personnel and the public during transportation accidents. Packaging durability increases as potential hazard of radioactive content increases.
- Very low levels of contained radioactive materials and low radiation levels outside packages result in low risks to people. Damaged packages may release measurable amounts of radioactive material, but the resulting risks are expected to be low.
- Some radioactive materials cannot be detected by commonly available instruments.
- Packages do not have RADIOACTIVE I, II, or III labels. Some may have EMPTY labels or may have the word "Radioactive" in the package marking.

FIRE OR EXPLOSION

- Some of these materials may burn, but most do not ignite readily.
- Many have cardboard outer packaging; content (physically large or small) can be of many different physical forms.
- Radioactivity does not change flammability or other properties of materials.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- **Priorities for rescue, life-saving, first aid, fire control and other hazards are higher than the priority for measuring radiation levels.**
- Radiation Authority must be notified of accident conditions. Radiation Authority is usually responsible for decisions about radiological consequences and closure of emergencies.
- Stay upwind, uphill and/or upstream.
- Keep unauthorized personnel away.
- Detain or isolate uninjured persons or equipment suspected to be contaminated; delay decontamination and cleanup until instructions are received from Radiation Authority.

PROTECTIVE CLOTHING

- Positive pressure self-contained breathing apparatus (SCBA) and structural firefighters' protective clothing will provide adequate protection.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 25 meters (75 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 100 meters (330 feet).

Fire

- When a large quantity of this material is involved in a major fire, consider an initial evacuation distance of 300 meters (1000 feet) in all directions.

EMERGENCY RESPONSE

FIRE

- Presence of radioactive material will not influence the fire control processes and should not influence selection of techniques.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Do not move damaged packages; move undamaged packages out of fire zone.

Small Fire

- Dry chemical, CO_2, water spray or regular foam.

Large Fire

- Water spray, fog (flooding amounts).

SPILL OR LEAK

- Do not touch damaged packages or spilled material.
- Cover liquid spill with sand, earth or other non-combustible absorbent material.
- Cover powder spill with plastic sheet or tarp to minimize spreading.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Medical problems take priority over radiological concerns.
- Use first aid treatment according to the nature of the injury.
- Do not delay care and transport of a seriously injured person.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Injured persons contaminated by contact with released material are not a serious hazard to health care personnel, equipment or facilities.

GUIDE 162 Radioactive Materials (Low to Moderate Level Radiation)

POTENTIAL HAZARDS

HEALTH

- Radiation presents minimal risk to transport workers, emergency response personnel and the public during transportation accidents. Packaging durability increases as potential hazard of radioactive content increases.
- Undamaged packages are safe. Contents of damaged packages may cause higher external radiation exposure, or both external and internal radiation exposure if contents are released.
- Low radiation hazard when material is inside container. If material is released from package or bulk container, hazard will vary from low to moderate. Level of hazard will depend on the type and amount of radioactivity, the kind of material it is in, and/or the surfaces it is on.
- Some material may be released from packages during accidents of moderate severity but risks to people are not great.
- Released radioactive materials or contaminated objects usually will be visible if packaging fails.
- Some exclusive use shipments of bulk and packaged materials will not have "RADIOACTIVE" labels. Placards, markings and shipping papers provide identification.
- Some packages may have a "RADIOACTIVE" label and a second hazard label. The second hazard is usually greater than the radiation hazard; so follow this GUIDE as well as the response GUIDE for the second hazard class label.
- Some radioactive materials cannot be detected by commonly available instruments.
- Runoff from control of cargo fire may cause low-level pollution.

FIRE OR EXPLOSION

- Some of these materials may burn, but most do not ignite readily.
- Uranium and Thorium metal cuttings may ignite spontaneously if exposed to air (see GUIDE 136).
- Nitrates are oxidizers and may ignite other combustibles (see GUIDE 141).

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- **Priorities for rescue, life-saving, first aid, fire control and other hazards are higher than the priority for measuring radiation levels.**
- Radiation Authority must be notified of accident conditions. Radiation Authority is usually responsible for decisions about radiological consequences and closure of emergencies.
- Stay upwind, uphill and/or upstream.
- Keep unauthorized personnel away.
- Detain or isolate uninjured persons or equipment suspected to be contaminated; delay decontamination and cleanup until instructions are received from Radiation Authority.

PROTECTIVE CLOTHING

- Positive pressure self-contained breathing apparatus (SCBA) and structural firefighters' protective clothing will provide adequate protection.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 25 meters (75 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 100 meters (330 feet).

Fire

- When a large quantity of this material is involved in a major fire, consider an initial evacuation distance of 300 meters (1000 feet) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- Presence of radioactive material will not influence the fire control processes and should not influence selection of techniques.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Do not move damaged packages; move undamaged packages out of fire zone.

Small Fire

- Dry chemical, CO_2, water spray or regular foam.

Large Fire

- Water spray, fog (flooding amounts).
- Dike runoff from fire control for later disposal.

SPILL OR LEAK

- Do not touch damaged packages or spilled material.
- Cover liquid spill with sand, earth or other non-combustible absorbent material.
- Dike to collect large liquid spills.
- Cover powder spill with plastic sheet or tarp to minimize spreading.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Medical problems take priority over radiological concerns.
- Use first aid treatment according to the nature of the injury.
- Do not delay care and transport of a seriously injured person.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- In case of contact with substance, wipe from skin immediately; flush skin or eyes with running water for at least 20 minutes.
- Injured persons contaminated by contact with released material are not a serious hazard to health care personnel, equipment or facilities.

GUIDE 163 Radioactive Materials (Low to High Level Radiation)

POTENTIAL HAZARDS

HEALTH

- Radiation presents minimal risk to transport workers, emergency response personnel and the public during transportation accidents. Packaging durability increases as potential hazard of radioactive content increases.
- Undamaged packages are safe. Contents of damaged packages may cause higher external radiation exposure, or both external and internal radiation exposure if contents are released.
- Type A packages (cartons, boxes, drums, articles, etc.) identified as "Type A" by marking on packages or by shipping papers contain non-life-endangering amounts. Partial releases might be expected if "Type A" packages are damaged in moderately severe accidents.
- Type B packages, and the rarely occurring Type C packages (large and small, usually metal), contain the most hazardous amounts. They can be identified by package markings or by shipping papers. Life-threatening conditions may exist only if contents are released or package shielding fails. Because of design, evaluation and testing of packages, these conditions would be expected only for accidents of utmost severity.
- The rarely occurring "Special Arrangement" shipments may be of Type A, Type B or Type C packages. Package type will be marked on packages, and shipment details will be on shipping papers.
- Radioactive White-I labels indicate radiation levels outside single, isolated, undamaged packages are very low (less than 0.005 mSv/h (0.5 mrem/h)).
- Radioactive Yellow-II and Yellow-III labeled packages have higher radiation levels. The transport index (TI) on the label identifies the maximum radiation level in mrem/h one meter from a single, isolated, undamaged package.
- Some radioactive materials cannot be detected by commonly available instruments.
- Water from cargo fire control may cause pollution.

FIRE OR EXPLOSION

- Some of these materials may burn, but most do not ignite readily.
- Radioactivity does not change flammability or other properties of materials.
- Type B packages are designed and evaluated to withstand total engulfment in flames at temperatures of 800°C (1475°F) for a period of 30 minutes.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- **Priorities for rescue, life-saving, first aid, fire control and other hazards are higher than the priority for measuring radiation levels.**
- Radiation Authority must be notified of accident conditions. Radiation Authority is usually responsible for decisions about radiological consequences and closure of emergencies.
- Stay upwind, uphill and/or upstream.
- Keep unauthorized personnel away.
- Detain or isolate uninjured persons or equipment suspected to be contaminated; delay decontamination and cleanup until instructions are received from Radiation Authority.

PROTECTIVE CLOTHING

- Positive pressure self-contained breathing apparatus (SCBA) and structural firefighters' protective clothing will provide adequate protection against internal radiation exposure, but not external radiation exposure.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 25 meters (75 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 100 meters (330 feet).

Fire

- When a large quantity of this material is involved in a major fire, consider an initial evacuation distance of 300 meters (1000 feet) in all directions.

EMERGENCY RESPONSE

FIRE

- Presence of radioactive material will not influence the fire control processes and should not influence selection of techniques.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Do not move damaged packages; move undamaged packages out of fire zone.

Small Fire

- Dry chemical, CO_2, water spray or regular foam.

Large Fire

- Water spray, fog (flooding amounts).
- Dike runoff from fire control for later disposal.

SPILL OR LEAK

- Do not touch damaged packages or spilled material.
- Damp surfaces on undamaged or slightly damaged packages are seldom an indication of packaging failure. Most packaging for liquid content have inner containers and/or inner absorbent materials.
- Cover liquid spill with sand, earth or other non-combustible absorbent material.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Medical problems take priority over radiological concerns.
- Use first aid treatment according to the nature of the injury.
- Do not delay care and transport of a seriously injured person.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Injured persons contaminated by contact with released material are not a serious hazard to health care personnel, equipment or facilities.

GUIDE 164 Radioactive Materials (Special Form/ Low to High Level External Radiation)

POTENTIAL HAZARDS

HEALTH

- Radiation presents minimal risk to transport workers, emergency response personnel and the public during transportation accidents. Packaging durability increases as potential hazard of radioactive content increases.
- Undamaged packages are safe; contents of damaged packages may cause external radiation exposure, and much higher external exposure if contents (source capsules) are released.
- Contamination and internal radiation hazards are not expected, but not impossible.
- Type A packages (cartons, boxes, drums, articles, etc.) identified as "Type A" by marking on packages or by shipping papers contain non-life-endangering amounts. Radioactive sources may be released if "Type A" packages are damaged in moderately severe accidents.
- Type B packages, and the rarely occurring Type C packages, (large and small, usually metal) contain the most hazardous amounts. They can be identified by package markings or by shipping papers. Life-threatening conditions may exist only if contents are released or package shielding fails. Because of design, evaluation and testing of packages, these conditions would be expected only for accidents of utmost severity.
- Radioactive White-I labels indicate radiation levels outside single, isolated, undamaged packages are very low (less than 0.005 mSv/h (0.5 mrem/h)).
- Radioactive Yellow-II and Yellow-III labeled packages have higher radiation levels. The transport index (TI) on the label identifies the maximum radiation level in mrem/h one meter from a single, isolated, undamaged package.
- Radiation from the package contents, usually in durable metal capsules, can be detected by most radiation instruments.
- Water from cargo fire control is not expected to cause pollution.

FIRE OR EXPLOSION

- Packagings can burn completely without risk of content loss from sealed source capsule.
- Radioactivity does not change flammability or other properties of materials.
- Radioactive source capsules and Type B packages are designed and evaluated to withstand total engulfment in flames at temperatures of 800°C (1475°F) for a period of 30 minutes.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- **Priorities for rescue, life-saving, first aid, fire control and other hazards are higher than the priority for measuring radiation levels.**
- Radiation Authority must be notified of accident conditions. Radiation Authority is usually responsible for decisions about radiological consequences and closure of emergencies.
- Stay upwind, uphill and/or upstream.
- Keep unauthorized personnel away.
- Delay final cleanup until instructions or advice is received from Radiation Authority.

PROTECTIVE CLOTHING

- Positive pressure self-contained breathing apparatus (SCBA) and structural firefighters' protective clothing will provide adequate protection against internal radiation exposure, but not external radiation exposure.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 25 meters (75 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 100 meters (330 feet).

Fire

- When a large quantity of this material is involved in a major fire, consider an initial evacuation distance of 300 meters (1000 feet) in all directions.

EMERGENCY RESPONSE

FIRE

- Presence of radioactive material will not influence the fire control processes and should not influence selection of techniques.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Do not move damaged packages; move undamaged packages out of fire zone.

Small Fire

- Dry chemical, CO_2, water spray or regular foam.

Large Fire

- Water spray, fog (flooding amounts).

SPILL OR LEAK

- Do not touch damaged packages or spilled material.
- Damp surfaces on undamaged or slightly damaged packages are seldom an indication of packaging failure. Contents are seldom liquid. Content is usually a metal capsule, easily seen if released from package.
- If source capsule is identified as being out of package, **DO NOT TOUCH**. Stay away and await advice from Radiation Authority.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Medical problems take priority over radiological concerns.
- Use first aid treatment according to the nature of the injury.
- Do not delay care and transport of a seriously injured person.
- Persons exposed to special form sources are not likely to be contaminated with radioactive material.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Injured persons contaminated by contact with released material are not a serious hazard to health care personnel, equipment or facilities.

GUIDE 165 Radioactive Materials (Fissile/Low to High Level Radiation)

POTENTIAL HAZARDS

HEALTH

- Radiation presents minimal risk to transport workers, emergency response personnel and the public during transportation accidents. Packaging durability increases as potential radiation and criticality hazards of the content increase.
- Undamaged packages are safe. Contents of damaged packages may cause higher external radiation exposure, or both external and internal radiation exposure if contents are released.
- Type AF or IF packages, identified by package markings, do not contain life-threatening amounts of material. External radiation levels are low and packages are designed, evaluated and tested to control releases and to prevent a fission chain reaction under severe transport conditions.
- Type B(U)F, B(M)F and CF packages (identified by markings on packages or shipping papers) contain potentially life-endangering amounts. Because of design, evaluation and testing of packages, fission chain reactions are prevented and releases are not expected to be life-endangering for all accidents except those of utmost severity.
- The rarely occurring "Special Arrangement" shipments may be of Type AF, BF or CF packages. Package type will be marked on packages, and shipment details will be on shipping papers.
- The transport index (TI) shown on labels or a shipping paper might not indicate the radiation level at one meter from a single, isolated, undamaged package; instead, it might relate to controls needed during transport because of the fissile properties of the materials. Alternatively, the fissile nature of the contents may be indicated by a criticality safety index (CSI) on a special FISSILE label or on the shipping paper.
- Some radioactive materials cannot be detected by commonly available instruments.
- Water from cargo fire control is not expected to cause pollution.

FIRE OR EXPLOSION

- These materials are seldom flammable. Packages are designed to withstand fires without damage to contents.
- Radioactivity does not change flammability or other properties of materials.
- Type AF, IF, B(U)F, B(M)F and CF packages are designed and evaluated to withstand total engulfment in flames at temperatures of 800°C (1475°F) for a period of 30 minutes.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- **Priorities for rescue, life-saving, first aid, fire control and other hazards are higher than the priority for measuring radiation levels.** • Radiation Authority must be notified of accident conditions. Radiation Authority is usually responsible for decisions about radiological consequences and closure of emergencies.
- Stay upwind, uphill and/or upstream. • Keep unauthorized personnel away.
- Detain or isolate uninjured persons or equipment suspected to be contaminated; delay decontamination and cleanup until instructions are received from Radiation Authority.

PROTECTIVE CLOTHING

- Positive pressure self-contained breathing apparatus (SCBA) and structural firefighters' protective clothing will provide adequate protection against internal radiation exposure, but not external radiation exposure.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 25 meters (75 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 100 meters (330 feet).

Fire

- When a large quantity of this material is involved in a major fire, consider an initial evacuation distance of 300 meters (1000 feet) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- Presence of radioactive material will not influence the fire control processes and should not influence selection of techniques.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Do not move damaged packages; move undamaged packages out of fire zone.

Small Fire

- Dry chemical, CO_2, water spray or regular foam.

Large Fire

- Water spray, fog (flooding amounts).

SPILL OR LEAK

- Do not touch damaged packages or spilled material.
- Damp surfaces on undamaged or slightly damaged packages are seldom an indication of packaging failure. Most packaging for liquid content have inner containers and/or inner absorbent materials.

Liquid Spill

- Package contents are seldom liquid. If any radioactive contamination resulting from a liquid release is present, it probably will be low-level.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Medical problems take priority over radiological concerns.
- Use first aid treatment according to the nature of the injury.
- Do not delay care and transport of a seriously injured person.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Injured persons contaminated by contact with released material are not a serious hazard to health care personnel, equipment or facilities.

GUIDE 166 Radioactive Materials - Corrosive (Uranium Hexafluoride/Water-Sensitive)

POTENTIAL HAZARDS

HEALTH

- Radiation presents minimal risk to transport workers, emergency response personnel and the public during transportation accidents. Packaging durability increases as potential radiation and criticality hazards of the content increase.
- **Chemical hazard greatly exceeds radiation hazard.**
- Substance reacts with water and water vapor in air to form **toxic and corrosive hydrogen fluoride gas, hydrofluoric acid**, and an extremely irritating and corrosive, white-colored, water-soluble residue.
- If inhaled, may be fatal. • Direct contact causes burns to skin, eyes, and respiratory tract.
- Low-level radioactive material; very low radiation hazard to people.
- Runoff from control of cargo fire may cause low-level pollution.

FIRE OR EXPLOSION

- Substance does not burn. • The material may react violently with fuels.
- Product will decompose to produce toxic and/or corrosive fumes.
- Containers in protective overpacks (horizontal cylindrical shape with short legs for tie-downs), are identified with "AF", "B(U)F" or "H(U)" on shipping papers or by markings on the overpacks. They are designed and evaluated to withstand severe conditions including total engulfment in flames at temperatures of 800°C (1475°F) for a period of 30 minutes.
- Bare filled cylinders, identified with UN2978 as part of the marking (may also be marked H(U) or H(M)), may rupture in heat of engulfing fire; bare empty (except for residue) cylinders will not rupture in fires.
- Radioactivity does not change flammability or other properties of materials.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- **Priorities for rescue, life-saving, first aid, fire control and other hazards are higher than the priority for measuring radiation levels.**
- Radiation Authority must be notified of accident conditions. Radiation Authority is usually responsible for decisions about radiological consequences and closure of emergencies.
- Stay upwind, uphill and/or upstream. • Keep unauthorized personnel away.
- Detain or isolate uninjured persons or equipment suspected to be contaminated; delay decontamination and cleanup until instructions are received from Radiation Authority.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 25 meters (75 feet) in all directions.

Spill

- See Table 1 - Initial Isolation and Protective Action Distances.

Fire

- When a large quantity of this material is involved in a major fire, consider an initial evacuation distance of 300 meters (1000 feet) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- DO NOT USE WATER OR FOAM ON MATERIAL ITSELF.
- If it can be done safely, move undamaged containers away from the area around the fire.

Small Fire

- Dry chemical or CO_2.

Large Fire

- Water spray, fog or regular foam.
- Cool containers with flooding quantities of water until well after fire is out.
- If this is impossible, withdraw from area and let fire burn.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- Do not touch damaged packages or spilled material.
- DO NOT GET WATER INSIDE CONTAINERS.
- Without fire or smoke, leak will be evident by visible and irritating vapors and residue forming at the point of release.
- Use fine water spray to reduce vapors; do not put water directly on point of material release from container.
- Residue buildup may self-seal small leaks.
- Dike far ahead of spill to collect runoff water.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Medical problems take priority over radiological concerns.
- Use first aid treatment according to the nature of the injury.
- **In case of skin contact with hydrogen fluoride gas and/or Hydrofluoric acid**, if calcium gluconate gel is available, rinse 5 minutes, then apply gel. Otherwise, continue rinsing until medical treatment is available.
- Do not delay care and transport of a seriously injured person.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Effects of exposure (inhalation, ingestion or skin contact) to substance may be delayed.
- Keep victim calm and warm.

Page intentionally left blank

There are no materials that refer to this guide.

Page intentionally left blank

There are no materials that refer to this guide.

POTENTIAL HAZARDS

HEALTH

- **TOXIC; Extremely Hazardous.**
- Inhalation extremely dangerous; may be fatal.
- Contact with gas or liquefied gas may cause burns, severe injury and/or frostbite.
- Odorless, will not be detected by sense of smell.

FIRE OR EXPLOSION

- **EXTREMELY FLAMMABLE.**

CAUTION: Flame can be invisible. Use an alternate method of detection (thermal camera, broom handle, etc.)

- May be ignited by heat, sparks or flames.
- Containers may explode when heated.
- Vapor explosion and poison hazard indoors, outdoors or in sewers.
- Vapors from liquefied gas are initially heavier than air and spread along ground.
- Vapors may travel to source of ignition and flash back.
- Runoff may create fire or explosion hazard.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Many gases are heavier than air and will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.
- Always wear thermal protective clothing when handling refrigerated/cryogenic liquids.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 100 meters (330 feet) in all directions.

Spill

- See Table 1 - Initial Isolation and Protective Action Distances.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

EMERGENCY RESPONSE

FIRE

CAUTION: Flame can be invisible. Use an alternate method of detection (thermal camera, broom handle, etc.)

- **DO NOT EXTINGUISH A LEAKING GAS FIRE UNLESS LEAK CAN BE STOPPED.**

Small Fire

- Dry chemical, CO_2 or water spray.

Large Fire

- Water spray, fog or regular foam.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Do not direct water at source of leak or safety devices; icing may occur.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- All equipment used when handling the product must be grounded.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- Do not direct water at spill or source of leak.
- If possible, turn leaking containers so that gas escapes rather than liquid.
- Prevent entry into waterways, sewers, basements or confined areas.
- Isolate area until gas has dispersed.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- In case of contact with liquefied gas, thaw frosted parts with lukewarm water.
- Keep victim calm and warm.
- Keep victim under observation.
- Effects of contact or inhalation may be delayed.

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- Substance is transported in molten form at a temperature above 705°C (1300°F).
- Violent reaction with water; contact may cause an explosion or may produce a flammable gas.
- Will ignite combustible materials (wood, paper, oil, debris, etc.).
- Contact with nitrates or other oxidizers may cause an explosion.
- Contact with containers or other materials, including cold, wet or dirty tools, may cause an explosion.
- Contact with concrete will cause spalling and small pops.

HEALTH

- Contact causes severe burns to skin and eyes.
- Fire may produce irritating and/or toxic gases.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Stay upwind, uphill and/or upstream.
- Keep unauthorized personnel away.
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear flame-retardant structural firefighters' protective clothing, including faceshield, helmet and gloves, as this will provide limited thermal protection.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 50 meters (150 feet) in all directions.

EMERGENCY RESPONSE

FIRE

- **Do not use water, except in life-threatening situations and then only in a fine spray.**
- **Do not use halogenated extinguishing agents or foam.**
- Move combustibles out of path of advancing pool if you can do so without risk.
- Extinguish fires started by molten material by using appropriate method for the burning material; keep water, halogenated extinguishing agents and foam away from the molten material.

SPILL OR LEAK

- Do not touch or walk through spilled material.
- Do not attempt to stop leak, due to danger of explosion.
- Keep combustibles (wood, paper, oil, etc.) away from spilled material.
- Substance is very fluid, spreads quickly, and may splash. Do not try to stop it with shovels or other objects.
- Dike far ahead of spill; use dry sand to contain the flow of material.
- Where possible allow molten material to solidify naturally.
- Avoid contact even after material solidifies. Molten, heated and cold aluminum look alike; do not touch unless you know it is cold.
- Clean up under the supervision of an expert after material has solidified.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- For severe burns, immediate medical attention is required.
- Removal of solidified molten material from skin requires medical assistance.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.

GUIDE 170 Metals (Powders, Dusts, Shavings, Borings, Turnings, or Cuttings, etc.)

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- May react violently or explosively on contact with water.
- Some are transported in flammable liquids.
- May be ignited by friction, heat, sparks or flames.
- Some of these materials will burn with intense heat.
- Dusts or fumes may form explosive mixtures in air.
- Containers may explode when heated.
- May re-ignite after fire is extinguished.

HEALTH

- Oxides from metallic fires are a severe health hazard.
- Inhalation or contact with substance or decomposition products may cause severe injury or death.
- Fire may produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Stay upwind, uphill and/or upstream.
- Keep unauthorized personnel away.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Large Spill

- Consider initial downwind evacuation for at least 50 meters (160 feet).

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- **DO NOT USE WATER, FOAM OR CO_2.**
- Dousing metallic fires with water will generate hydrogen gas, an extremely dangerous explosion hazard, particularly if fire is in a confined environment (i.e., building, cargo hold, etc.).
- Use DRY sand, graphite powder, dry sodium chloride-based extinguishers, or class D extinguishers.
- Confining and smothering metal fires is preferable rather than applying water.
- If it can be done safely, move undamaged containers away from the area around the fire.

Fire Involving Tanks or Car/Trailer Loads

- If impossible to extinguish, protect surroundings and allow fire to burn itself out.

SPILL OR LEAK

- ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- Prevent entry into waterways, sewers, basements or confined areas.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- Some may burn but none ignite readily.
- Containers may explode when heated.
- Some may be transported hot.
- For UN3508, Capacitor, asymmetric, be aware of possible short circuiting as this product is transported in a charged state.
- Polymeric beads, expandable (UN2211) may evolve flammable vapours.

HEALTH

- Inhalation of material may be harmful.
- Contact may cause burns to skin and eyes.
- Inhalation of Asbestos dust may have a damaging effect on the lungs.
- Fire may produce irritating, corrosive and/or toxic gases.
- Some liquids produce vapors that may cause dizziness or asphyxiation.
- Runoff from fire control or dilution water may cause environmental contamination.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area in all directions for at least 50 meters (150 feet) for liquids and at least 25 meters (75 feet) for solids.

Spill

- For highlighted materials: see Table 1 - Initial Isolation and Protective Action Distances.
- For non-highlighted materials: increase the immediate precautionary measure distance, in the downwind direction, as necessary.

Fire

- If tank, rail car or tank truck is involved in a fire, ISOLATE for 800 meters (1/2 mile) in all directions; also, consider initial evacuation for 800 meters (1/2 mile) in all directions.

EMERGENCY RESPONSE

FIRE

Small Fire

- Dry chemical, CO_2, water spray or regular foam.

Large Fire

- Water spray, fog or regular foam.
- Do not scatter spilled material with high-pressure water streams.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Dike runoff from fire control for later disposal.

Fire Involving Tanks

- Cool containers with flooding quantities of water until well after fire is out.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- Prevent dust cloud.
- For Asbestos, avoid inhalation of dust. Cover spill with plastic sheet or tarp to minimize spreading. Do not clean up or dispose of, except under supervision of a specialist.

Small Dry Spill

- With clean shovel, place material into clean, dry container and cover loosely; move containers from spill area.

Small Spill

- Pick up with sand or other non-combustible absorbent material and place into containers for later disposal.

Large Spill

- Dike far ahead of liquid spill for later disposal.
- Cover powder spill with plastic sheet or tarp to minimize spreading.
- Prevent entry into waterways, sewers, basements or confined areas.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.

POTENTIAL HAZARDS

HEALTH

- Inhalation of vapors or contact with substance will result in contamination and potential harmful effects.
- Fire will produce irritating, corrosive and/or toxic gases.

FIRE OR EXPLOSION

- Non-combustible, substance itself does not burn but may react upon heating to produce corrosive and/or toxic fumes.
- Runoff may pollute waterways.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Stay upwind, uphill and/or upstream.
- Keep unauthorized personnel away.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 50 meters (150 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 100 meters (330 feet).

Fire

- When any large container is involved in a fire, consider initial evacuation for 500 meters (1/3 mile) in all directions.

EMERGENCY RESPONSE

FIRE

- Use extinguishing agent suitable for type of surrounding fire.
- **Do not direct water at the heated metal.**

SPILL OR LEAK

- Do not touch or walk through spilled material.
- Do not touch damaged containers or spilled material unless wearing appropriate protective clothing.
- Stop leak if you can do it without risk.
- Prevent entry into waterways, sewers, basements or confined areas.
- Do not use steel or aluminum tools or equipment.
- Cover with earth, sand or other non-combustible material followed with plastic sheet to minimize spreading or contact with rain.
- For mercury, use a mercury spill kit.
- Mercury spill areas may be subsequently treated with calcium sulphide/calcium sulfide or with sodium thiosulphate/sodium thiosulfate wash to neutralize any residual mercury.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- Keep victim calm and warm.

GUIDE 173 Adsorbed Gases - Toxic*

POTENTIAL HAZARDS

HEALTH

- **TOXIC; may be fatal if inhaled or absorbed through skin.**
- Vapors may be irritating.
- Contact with gas may cause burns and injury.
- Fire will produce irritating, corrosive and/or toxic gases.
- Runoff from fire control or dilution water may cause environmental contamination.

FIRE OR EXPLOSION

- Some gases may burn or be ignited by heat, sparks or flames.
- May form explosive mixtures with air.
- Oxidizers may ignite combustibles (wood, paper, oil, clothing, etc.) but NOT readily due to low transportation pressures.
- Vapors may travel to source of ignition and flash back.
- Some of these materials may react violently with water.
- Cylinders exposed to fire may vent and release toxic and flammable gas through pressure relief devices.
- Runoff may create fire hazard.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Many gases are heavier than air and will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Wear chemical protective clothing that is specifically recommended by the manufacturer **when there is NO RISK OF FIRE**.
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 100 meters (330 feet) in all directions.

Spill

- See Table 1 - Initial Isolation and Protective Action Distances.

Fire

- If several small packages (inside a railcar or trailer) are involved in a fire, ISOLATE for 1600 meters (1 mile) in all directions; also, consider initial evacuation for 1600 meters (1 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

*** Some substances may also be flammable, corrosive and/or oxidizing**

EMERGENCY RESPONSE

FIRE

- **DO NOT EXTINGUISH A LEAKING GAS FIRE UNLESS LEAK CAN BE STOPPED.**

Small Fire

- Dry chemical, CO_2, water spray or alcohol-resistant foam.
- **For UN3515, UN3518, UN3520**, use water only; no dry chemical, CO_2 or Halon®.

Large Fire

- Water spray, fog or alcohol-resistant foam.
- Do not get water inside containers.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Damaged cylinders should be handled only by specialists.

Fire Involving Several Small Packages (inside a railcar or trailer)

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Do not direct water at source of leak or safety devices.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.

SPILL OR LEAK

- Some gases may be flammable. ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- For flammable gases, all equipment used when handling the product must be grounded.
- For oxidizing substances, keep combustibles (wood, paper, oil, etc.) away from spilled material.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- Do not direct water at spill or source of leak.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- Prevent entry into waterways, sewers, basements or confined areas.
- Isolate area until gas has dispersed.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- **Do not perform mouth-to-mouth resuscitation if victim ingested or inhaled the substance; wash face and mouth before giving artificial respiration. Use a pocket mask equipped with a one-way valve or other proper respiratory medical device.**
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of contact with substance, immediately flush skin or eyes with running water for at least 20 minutes.
- In case of burns, immediately cool affected skin for as long as possible with cold water. Do not remove clothing if adhering to skin.
- Keep victim calm and warm.
- Keep victim under observation.
- Effects of contact or inhalation may be delayed.

GUIDE 174 Adsorbed Gases - Flammable or Oxidizing

POTENTIAL HAZARDS

FIRE OR EXPLOSION

- Some gases will be ignited by heat, sparks or flames.
- Substance does not burn but will support combustion.
- Vapors may travel to source of ignition and flash back.
- Cylinders exposed to fire may vent and release flammable gas through pressure relief devices.
- Containers may explode when exposed to prolonged direct flame impingement.

HEALTH

- Vapors may cause dizziness or asphyxiation without warning.
- Some may be irritating if inhaled at high concentrations.
- Contact with gas may cause burns and injury.
- Fire may produce irritating and/or toxic gases.

PUBLIC SAFETY

- **CALL 911. Then call emergency response telephone number on shipping paper.** If shipping paper not available or no answer, refer to appropriate telephone number listed on the inside back cover.
- Keep unauthorized personnel away.
- Stay upwind, uphill and/or upstream.
- Many gases are heavier than air and will spread along the ground and collect in low or confined areas (sewers, basements, tanks, etc.).
- Ventilate closed spaces before entering, but only if properly trained and equipped.

PROTECTIVE CLOTHING

- Wear positive pressure self-contained breathing apparatus (SCBA).
- Structural firefighters' protective clothing provides thermal protection **but only limited chemical protection**.

EVACUATION

Immediate precautionary measure

- Isolate spill or leak area for at least 100 meters (330 feet) in all directions.

Large Spill

- Consider initial downwind evacuation for at least 800 meters (1/2 mile).

Fire

- If several small packages (inside a railcar or trailer) are involved in a fire, ISOLATE for 1600 meters (1 mile) in all directions; also, consider initial evacuation for 1600 meters (1 mile) in all directions.



In Canada, an Emergency Response Assistance Plan (ERAP) may be required for this product. Please consult the shipping paper and/or the ERAP Program Section (page 390).

EMERGENCY RESPONSE

FIRE

- **DO NOT EXTINGUISH A LEAKING GAS FIRE UNLESS LEAK CAN BE STOPPED.**
- Use extinguishing agent suitable for type of surrounding fire.

Small Fire

- Dry chemical or CO_2.

Large Fire

- Water spray or fog.
- If it can be done safely, move undamaged containers away from the area around the fire.
- Damaged cylinders should be handled only by specialists.

Fire Involving Several Small Packages (inside a railcar or trailer)

- Fight fire from maximum distance or use unmanned master stream devices or monitor nozzles.
- Cool containers with flooding quantities of water until well after fire is out.
- Do not direct water at source of leak or safety devices.
- Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.
- ALWAYS stay away from tanks engulfed in fire.
- For massive fire, use unmanned master stream devices or monitor nozzles; if this is impossible, withdraw from area and let fire burn.

SPILL OR LEAK

- For flammable gases, ELIMINATE all ignition sources (no smoking, flares, sparks or flames) from immediate area.
- For oxidizing substances, keep combustibles (wood, paper, oil, etc.) away from spilled material.
- All equipment used when handling the product must be grounded.
- Do not touch or walk through spilled material.
- Stop leak if you can do it without risk.
- Use water spray to reduce vapors or divert vapor cloud drift. Avoid allowing water runoff to contact spilled material.
- Do not direct water at spill or source of leak.
- Prevent spreading of vapors through sewers, ventilation systems and confined areas.
- Ventilate the area.
- Isolate area until gas has dispersed.

FIRST AID

- Call 911 or emergency medical service.
- Ensure that medical personnel are aware of the material(s) involved and take precautions to protect themselves.
- Move victim to fresh air if it can be done safely.
- Give artificial respiration if victim is not breathing.
- Administer oxygen if breathing is difficult.
- Remove and isolate contaminated clothing and shoes.
- In case of burns, immediately cool affected skin for as long as possible with cold water. Do not remove clothing if adhering to skin.
- Keep victim calm and warm.

INTRODUCTION TO GREEN TABLES

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

This table suggests distances useful to protect people from vapors/gases resulting from spills involving:

- materials that are considered toxic by inhalation (TIH) (PIH in the US)
- materials that produce toxic gases upon contact with water
- chemical warfare agents

This table provides first responders with initial guidance until technically qualified emergency response personnel are available. For each material, first responders will find distances for the following zones:

- The **Initial Isolation Zone** defines an area **surrounding** the incident in which people may be exposed to dangerous (upwind) and life-threatening (downwind) concentrations of material.
- The **Protective Action Zone** defines an area **downwind** from the incident in which people may become incapacitated and unable to take protective action and/or incur serious or irreversible health effects. Table 1 provides specific guidance for small and large spills occurring day or night.

Adjusting distances for a specific incident involves many interdependent variables. These adjustments should only be made by technically qualified personnel. For this reason, no precise guidance can be provided in this document to aid in adjusting the table distances; however, general guidance follows.

Factors that May Change the Protective Action Distances

Fire

In the **orange-bordered pages**, under **EVACUATION – Fire**, the evacuation distance required to protect against fragmentation hazard of a large container is clearly indicated. If involved in a fire, the toxic hazard may be less dangerous than the fire or explosion hazard.

In these cases, the **fire hazard distance should be used** as an isolation distance and Table 1 should be used to protect downwind for residual material release.

Worst-case scenario: terrorism, sabotage or catastrophic accident

Initial isolation and protective action distances are derived from historical data on transportation incidents and the use of statistical models. For worst-case scenarios involving the instantaneous release of the entire contents of a package (e.g., as a result of terrorism, sabotage or catastrophic accident), the distances may increase substantially.

For such events, **doubling** the initial isolation and protective action distances is appropriate in absence of other information.

When more than one large package is leaking

If more than one rail car, tank truck, tank or large cylinder, containing TIH materials is leaking, **large spill** distances may need to be increased.

Other factors that can increase the protective action distance:

- If a material has a **protective action distance of 11.0+ km (7.0+ miles)**, the actual distance can be larger in certain atmospheric conditions.
- If the material's vapor plume is **channeled in a valley** or **between many tall buildings**, protective action distances may be larger than shown due to less mixing of the plume with the atmosphere.
- If there is a **daytime spill** in a region with known **strong temperature inversions** or **snow cover**, or it occurs **near sunset**, this may require an increase of the protective action distance because airborne contaminants mix and disperse more slowly and may travel much farther downwind.
  - › In such cases, the nighttime protective action distances may be more appropriate.
- If the temperature of the **liquid spill** or the **outdoor temperature exceeds 30°C (86°F)**, the protective action distance may be larger.

Water-reactive materials

Materials that react with water to produce large amounts of toxic gases are included in Table 1. Some of these materials have 2 entries in Table 1. They are identified by **(when spilled on land)** since they are TIH products and **(when spilled in water)** because they produce additional toxic gases when spilled in water.

Choose the **larger protective action distance** if:

- it is not clear whether the spill is on land or in water
- the spill occurs both on land and in water

TABLE 2 - WATER-REACTIVE MATERIALS WHICH PRODUCE TOXIC GASES

This table lists materials that produce large amounts of Toxic Inhalation Hazard gases (TIH) when spilled in water as well as the TIH gases that are produced.

NOTE: The produced TIH gases indicated in Table 2 are for information purposes only. In Table 1, the initial isolation and protective action distances have already taken into consideration the produced TIH gas.

When a water-reactive TIH-producing material is spilled into a river or stream, the source of the toxic gas may flow downstream for a great distance.

TABLE 3 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES FOR LARGE SPILLS FOR DIFFERENT QUANTITIES OF SIX COMMON TIH (PIH IN THE US) GASES

This table lists materials that may be more commonly encountered. These materials are:

- UN1005 - Ammonia, anhydrous
- UN1017 - Chlorine
- UN1040 - Ethylene oxide and UN1040 - Ethylene oxide with nitrogen

- UN1050 - Hydrogen chloride, anhydrous and UN2186 - Hydrogen chloride, refrigerated liquid
- UN1052 - Hydrogen fluoride, anhydrous
- UN1079 - Sulfur dioxide/Sulphur dioxide

This table provides initial isolation and protective action distances for large spills (more than 208 liters or 55 US gallons):

- involving different container types (therefore different volume capacities)
- for daytime and nighttime situations
- for different wind speeds (low, moderate and high)

PROTECTIVE ACTIONS

Protective actions are the steps taken to preserve the health and safety of emergency responders and the public during an incident involving releases of hazardous materials/ dangerous goods.

Table 1 - Initial Isolation and Protective Action Distances (green-bordered pages) predicts the size of the area that could be affected by a cloud of toxic gas. People in this area should be evacuated and/or sheltered-in-place inside buildings.

Isolate hazard area and deny entry means to keep everybody away from the area if they are not directly involved in emergency response operations. Unprotected emergency responders should not be allowed to enter the isolation zone.

This "isolation" task is done to establish control over the area of operations. This is the first step for any protective actions that may follow.

Evacuate means to move all people from a threatened area to a safer place. To perform an evacuation, there must be enough time for people to be warned, get ready, and leave an area. If there is enough time, evacuation is the best protective action.

Begin evacuating people nearby and those who are outdoors in direct view of the scene. When additional help arrives, expand the area to be evacuated downwind and crosswind to at least the extent recommended in this guidebook.

Even after people move to the distances recommended, they may not be completely safe from harm. They should not be permitted to gather at such distances. Send evacuees to a definite place, by a specific route, far enough away so they will not have to be moved again if the wind shifts.

Shelter-in-place means people should seek shelter inside a building and remain inside until the danger passes. **It is vital for first responders to maintain communications with sheltered-in-place people** so that they are advised about changing conditions.

Sheltering-in-place is used either when:

- evacuating the public would cause greater risk than staying where they are
- an evacuation cannot be performed

Direct the people inside to:

- close all doors and windows
- shut off all ventilating, heating and cooling systems
- stay far from windows to avoid shattered glass and projectile metal fragments in the event of a fire and/or explosion
- tune in to local radio or TV stations, and stay inside until told it is safe to leave by first responders

Shelter-in-place may not be the best option if:

- the vapors are flammable

- it will take a long time for the gas to clear the area
- buildings cannot be closed tightly

Vehicles can offer some protection for a short period if the windows are closed and the ventilation systems are shut off. Vehicles are not as effective as buildings for in-place protection.

NOTE: Every hazardous materials/dangerous goods incident is different. Each will have special problems and concerns. Actions to protect the public must be carefully selected. These pages can help with **initial** decisions on how to protect the public. Officials must continue to gather information and monitor the situation until the threat is removed.

PROTECTIVE ACTION DECISION FACTORS TO CONSIDER

The choice of protective actions for a given situation depends on a number of factors. For some cases, evacuation may be the best option; in others, sheltering-in-place may be the best course. Sometimes, these two actions may be used in combination. In any emergency, officials need to quickly give the public instructions. The public will need continuing information and instructions while being evacuated or sheltered-in-place.

Proper evaluation of the factors listed below will determine the effectiveness of evacuation or in-place protection (shelter-in-place). The importance of these factors can vary with emergency conditions. In specific emergencies, other factors may need to be identified and considered as well. This list indicates what kind of information may be needed to make the initial decision.

The hazardous materials/dangerous goods:

- degree of health hazard
- chemical and physical properties
- amount involved
- containment/control of release
- rate of vapor movement

The population threatened:

- location
- number of people
- time available to evacuate or shelter-in-place
- ability to control evacuation or shelter-in-place
- building types and availability
- special institutions or populations, e.g., nursing homes, hospitals, prisons

The weather conditions:

- effect on vapor and cloud movement
- potential for change
- effect on evacuation or shelter-in-place

BACKGROUND ON TABLE 1 – INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

Initial isolation and protective action distances in this guidebook were determined for small and large spills occurring during day or night. The overall analysis, statistical in nature, was conducted using:

- state-of-the-art emission rate and dispersion models
- statistical release data from the U.S. Department of Transportation (DOT) Hazardous Materials Information System (HMIS) database
- meteorological observations from more than 120 locations in the United States, Canada, and Mexico
- the most current toxicological exposure guidelines

For each chemical, thousands of hypothetical releases were modeled to account for the statistical variance in both release amount and atmospheric conditions. Based on this statistical sample, they selected the 90th percentile protective action distance for each chemical and category to appear in the table. A brief description of the analysis is provided below.

A detailed report outlining the methodology and data used to generate the initial isolation and protective action distances may be obtained from the U.S. DOT, Pipeline and Hazardous Materials Safety Administration (PHMSA).

DESCRIPTION OF THE ANALYSIS

Release amounts and emission rates into the atmosphere were statistically modeled based on:

- data from the U.S. DOT HMIS database
- container types and sizes authorized for transport as specified in 49 CFR §172.101 and Part 173
- physical properties of the individual materials
- atmospheric data from a historical database

For liquefied gases, which can flash to form both a vapor/aerosol mixture and an evaporating pool, the emission model calculated one or both of:

- the release of vapor due to evaporation of pools on the ground
- direct release of vapors from the container

The emission model also calculated the emission of toxic vapor by-products generated from spilling water-reactive materials in water.

Small spills involve 208 liters (55 US gallons) or less.

Large spills involve greater quantities.

The exceptions are the entries at the beginning of Table 1 marked **(when used as a weapon)**. The volumes used for these calculations varies, but in most cases:

- Small spills include releases up to 2 kg (4.4 lbs.).
- Large spills include releases up to 25 kg (55 lbs.).

Downwind dispersion of the vapor was estimated for each case modeled. Using a database containing hourly meteorological data from 120 American, Canadian, and Mexican cities, the atmospheric parameters affecting the dispersion and the emission rate were selected.

The dispersion calculation accounted for both the:

- time-dependent emission rate from the source
- density of the vapor plume (i.e., heavy gas effects)

Since atmospheric mixing is less effective at dispersing vapor plumes during nighttime, day and night were separated in the analysis.

In the table:

- **day** refers to time periods after sunrise and before sunset
- **night** includes all hours between sunset and sunrise

Toxicological short-term exposure guidelines for the materials were applied to determine the downwind distance to which people may:

- become incapacitated and unable to take protective action
- incur serious health effects after a single, or rare, exposure

When available, toxicological exposure guidelines were chosen from AEGL-2 or ERPG-2 emergency response guidelines. AEGL-2 values were the first choice.

For materials without AEGL-2 or ERPG-2 values, emergency response guidelines were estimated based on lethal concentration limits derived from animal-based-studies. This approach was recommended by an independent panel of toxicological experts from industry and academia.

HOW TO USE TABLE 1 – INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

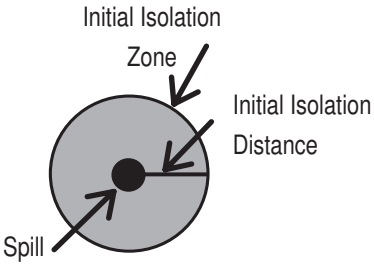
(1) The responder should already have:

- identified the material by its ID number and name (if you cannot find an ID number, use the Name of Material index in the blue-bordered pages to find that number);
- confirmed that the material is highlighted in green in the yellow or blue-bordered pages. If not, Table 1 doesn't apply;
- found the three-digit guide for the material, in order to consult emergency actions it recommends along with this table; and
- **noted the wind direction**

(2) Look in Table 1 (green-bordered pages) for the ID number and name of the material involved. Some ID numbers have more than one shipping name listed. Look for the specific name of the material. If you do not know the shipping name and Table 1 lists more than one name for the same ID number, use the entry with the largest distances.

(3) Determine if the incident involves a SMALL or LARGE spill and if it is DAY or NIGHT. A SMALL SPILL consists of a release of 208 liters (55 US gallons) or less. This generally corresponds to a spill from a single small package (for example, a drum), a small cylinder, or a small leak from a large package. A LARGE SPILL consists of a release of more than 208 liters (55 US gallons). This usually involves a spill from a large package, or multiple spills from many small packages. DAY is any time after sunrise and before sunset. NIGHT is any time between sunset and sunrise.

(4) Look up the INITIAL ISOLATION DISTANCE. This distance defines the radius of a zone (initial isolation zone) surrounding the spill in ALL DIRECTIONS. In this zone, protective clothing and respiratory protection is required. Evacuate the general public in a direction perpendicular to wind direction (crosswind) and away from the spill.

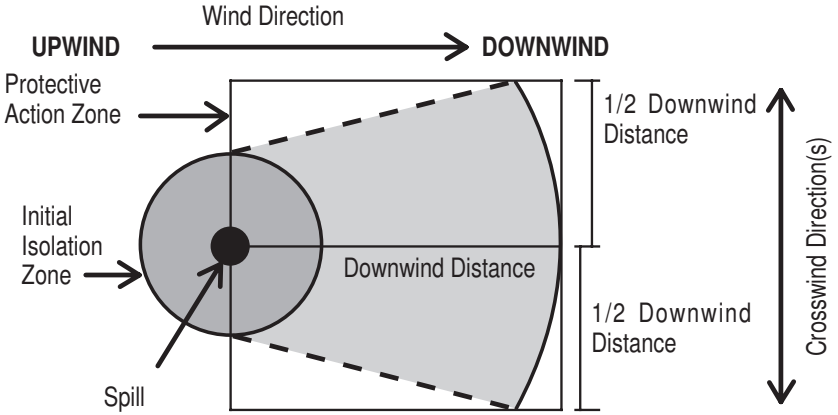


(5) Look up the PROTECTIVE ACTION DISTANCE.
For a given material, spill size, and whether day or night, Table 1 gives the downwind distance—in kilometers and miles—from the spill or leak source, for which you should consider protective actions. For practical purposes, the protective action zone (i.e., the area in which people are at risk of harmful exposure) is a square. Its length and width are the same as the downwind distance shown in Table 1. Protective actions are the

steps you take to preserve the health and safety of emergency responders and the public. People in this area should be evacuated and/or sheltered-in-place. Consult pages 289-291.

(6) Initiate protective actions beginning with those closest to the spill site and working away in a downwind direction. When a water-reactive TIH (PIH in the US) producing material is spilled into a river or stream, the source of the toxic gas may move with the current or stretch from the spill point downstream for a large distance.

In the figure below, the spill is located at the center of the small black circle. The larger circle represents the initial isolation zone around the spill. The square (the protective action zone) is the area in which you should take protective actions.



Note 1: For factors that may change the protective action distances, see "Introduction to Green Tables" (page 286).

Note 2: When a product in Table 1 has the mention (when spilled in water), you can refer to Table 2 for the list of gases produced when these materials are spilled in water. The TIH gases indicated in Table 2 are for information purposes only.

For more information on the material, safety precautions and mitigation procedures, call the emergency response telephone number listed on the shipping paper or the appropriate response agency as soon as possible.

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
——	117	AC **(when used as a weapon)**	60 m (200 ft)	0.3 km (0.2 mi)	1.0 km (0.6 mi)	1000 m (3000 ft)	3.7 km (2.3 mi)	8.4 km (5.3 mi)
——	154	Adamsite **(when used as a weapon)**	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)	60 m (200 ft)	0.3 km (0.2 mi)	1.4 km (0.9 mi)
——	153	Buzz **(when used as a weapon)**	60 m (200 ft)	0.4 km (0.2 mi)	1.7 km (1.1 mi)	400 m (1250 ft)	2.2 km (1.4 mi)	8.1 km (5.0 mi)
——	153	BZ **(when used as a weapon)**	60 m (200 ft)	0.4 km (0.2 mi)	1.7 km (1.1 mi)	400 m (1250 ft)	2.2 km (1.4 mi)	8.1 km (5.0 mi)
——	159	CA **(when used as a weapon)**	30 m (100 ft)	0.1 km (0.1 mi)	0.4 km (0.3 mi)	100 m (300 ft)	0.5 km (0.4 mi)	2.6 km (1.6 mi)
——	125	CG **(when used as a weapon)**	150 m (500 ft)	0.8 km (0.5 mi)	3.2 km (2.0 mi)	1000 m (3000 ft)	7.5 km (4.7 mi)	11.0+ km (7.0+ mi)
——	125	CK **(when used as a weapon)**	30 m (100 ft)	0.2 km (0.2 mi)	1.4 km (0.9 mi)	300 m (1000 ft)	1.4 km (0.9 mi)	6.1 km (3.8 mi)
——	153	CN **(when used as a weapon)**	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	60 m (200 ft)	0.3 km (0.2 mi)	1.2 km (0.8 mi)
——	153	CS **(when used as a weapon)**	30 m (100 ft)	0.1 km (0.1 mi)	0.6 km (0.4 mi)	100 m (300 ft)	0.4 km (0.3 mi)	1.9 km (1.2 mi)
——	154	CX **(when used as a weapon)**	60 m (200 ft)	0.2 km (0.2 mi)	1.1 km (0.7 mi)	200 m (600 ft)	1.2 km (0.7 mi)	5.1 km (3.2 mi)
——	151	DA **(when used as a weapon)**	30 m (100 ft)	0.2 km (0.1 mi)	0.8 km (0.5 mi)	300 m (1000 ft)	1.9 km (1.2 mi)	7.5 km (4.7 mi)
——	153	DC **(when used as a weapon)**	30 m (100 ft)	0.1 km (0.1 mi)	0.6 km (0.4 mi)	60 m (200 ft)	0.4 km (0.3 mi)	1.8 km (1.1 mi)
——	154	DM **(when used as a weapon)**	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)	60 m (200 ft)	0.3 km (0.2 mi)	1.4 km (0.9 mi)
——	125	DP **(when used as a weapon)**	30 m (100 ft)	0.2 km (0.1 mi)	0.7 km (0.4 mi)	200 m (600 ft)	1.0 km (0.7 mi)	2.4 km (1.5 mi)
——	151	ED **(when used as a weapon)**	150 m (500 ft)	0.9 km (0.6 mi)	2.1 km (1.3 mi)	1000 m (3000 ft)	5.9 km (3.7 mi)	8.3 km (5.2 mi)
——	153	GA **(when used as a weapon)**	30 m (100 ft)	0.2 km (0.1 mi)	0.2 km (0.1 mi)	100 m (300 ft)	0.5 km (0.4 mi)	0.6 km (0.4 mi)

—	153	GB **(when used as a weapon)**	60 m	(200 ft)	0.4 km	(0.3 mi)	1.1 km	(0.7 mi)	400 m	(1250 ft)	2.1 km	(1.3 mi)	4.9 km	(3.0 mi)
—	153	GD **(when used as a weapon)**	60 m	(200 ft)	0.4 km	(0.3 mi)	0.7 km	(0.5 mi)	300 m	(1000 ft)	1.8 km	(1.1 mi)	2.7 km	(1.7 mi)
—	153	GF **(when used as a weapon)**	30 m	(100 ft)	0.2 km	(0.2 mi)	0.3 km	(0.2 mi)	150 m	(500 ft)	0.8 km	(0.5 mi)	1.0 km	(0.6 mi)
—	153	H **(when used as a weapon)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	60 m	(200 ft)	0.3 km	(0.2 mi)	0.4 km	(0.3 mi)
—	153	HD **(when used as a weapon)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	60 m	(200 ft)	0.3 km	(0.2 mi)	0.4 km	(0.3 mi)
—	153	HL **(when used as a weapon)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	100 m	(300 ft)	0.5 km	(0.3 mi)	1.0 km	(0.6 mi)
—	153	HN-1 **(when used as a weapon)**	60 m	(200 ft)	0.3 km	(0.2 mi)	0.5 km	(0.3 mi)	200 m	(600 ft)	1.1 km	(0.7 mi)	1.8 km	(1.1 mi)
—	153	HN-2 **(when used as a weapon)**	60 m	(200 ft)	0.3 km	(0.2 mi)	0.6 km	(0.4 mi)	300 m	(1000 ft)	1.3 km	(0.8 mi)	2.1 km	(1.3 mi)
—	153	HN-3 **(when used as a weapon)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	60 m	(200 ft)	0.3 km	(0.2 mi)	0.3 km	(0.2 mi)
—	153	L (Lewisite) **(when used as a weapon)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	100 m	(300 ft)	0.5 km	(0.3 mi)	1.0 km	(0.6 mi)
—	153	Lewisite **(when used as a weapon)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	100 m	(300 ft)	0.5 km	(0.3 mi)	1.0 km	(0.6 mi)
—	152	MD **(when used as a weapon)**	300 m	(1000 ft)	1.6 km	(1.0 mi)	4.3 km	(2.7 mi)	1000 m	(3000 ft)	11.0+ km	(7.0+ mi)	11.0+ km	(7.0+ mi)
—	153	Mustard **(when used as a weapon)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	60 m	(200 ft)	0.3 km	(0.2 mi)	0.4 km	(0.3 mi)
—	153	Mustard Lewisite **(when used as a weapon)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	100 m	(300 ft)	0.5 km	(0.3 mi)	1.0 km	(0.6 mi)
—	152	PD **(when used as a weapon)**	60 m	(200 ft)	0.4 km	(0.3 mi)	0.4 km	(0.3 mi)	300 m	(1000 ft)	1.6 km	(1.0 mi)	1.6 km	(1.0 mi)
—	119	SA **(when used as a weapon)**	300 m	(1000 ft)	1.9 km	(1.2 mi)	5.7 km	(3.6 mi)	1000 m	(3000 ft)	8.9 km	(5.6 mi)	11.0+ km	(7.0+ mi)
—	153	Sarin **(when used as a weapon)**	60 m	(200 ft)	0.4 km	(0.3 mi)	1.1 km	(0.7 mi)	400 m	(1250 ft)	2.1 km	(1.3 mi)	4.9 km	(3.0 mi)

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
——	**153**	Soman **(when used as a weapon)**	60 m (200 ft)	0.4 km (0.3 mi)	0.7 km (0.5 mi)	300 m (1000 ft)	1.8 km (1.1 mi)	2.7 km (1.7 mi)
——	**153**	Tabun **(when used as a weapon)**	30 m (100 ft)	0.2 km (0.1 mi)	0.2 km (0.1 mi)	100 m (300 ft)	0.5 km (0.4 mi)	0.6 km (0.4 mi)
——	**153**	Thickened GD **(when used as a weapon)**	60 m (200 ft)	0.4 km (0.3 mi)	0.7 km (0.5 mi)	300 m (1000 ft)	1.8 km (1.1 mi)	2.7 km (1.7 mi)
——	**153**	VX **(when used as a weapon)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	60 m (200 ft)	0.4 km (0.2 mi)	0.3 km (0.2 mi)
1005 1005	**125** **125**	Ammonia, anhydrous Anhydrous ammonia	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	**Refer to table 3**		
1008 1008	**125** **125**	Boron trifluoride Boron trifluoride, compressed	30 m (100 ft)	0.2 km (0.1 mi)	0.7 km (0.5 mi)	400 m (1250 ft)	2.3 km (1.4 mi)	5.1 km (3.2 mi)
1016 1016	**119** **119**	Carbon monoxide Carbon monoxide, compressed	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	200 m (600 ft)	1.2 km (0.7 mi)	4.3 km (2.7 mi)
1017	**124**	Chlorine	60 m (200 ft)	0.3 km (0.2 mi)	1.4 km (0.9 mi)	**Refer to table 3**		
1026	**119**	Cyanogen	30 m (100 ft)	0.1 km (0.1 mi)	0.4 km (0.3 mi)	60 m (200 ft)	0.3 km (0.2 mi)	1.1 km (0.7 mi)
1040 1040	**119P** **119P**	Ethylene oxide Ethylene oxide with Nitrogen	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.2 mi)	**Refer to table 3**		
1045 1045	**124** **124**	Fluorine Fluorine, compressed	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	100 m (300 ft)	0.5 km (0.3 mi)	2.3 km (1.4 mi)
1048	**125**	Hydrogen bromide, anhydrous	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.2 mi)	150 m (500 ft)	1.0 km (0.6 mi)	3.4 km (2.1 mi)
1050	**125**	Hydrogen chloride, anhydrous	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)	**Refer to table 3**		

1051	**117P**	Hydrogen cyanide, anhydrous, stabilized	60 m	(200 ft)	0.2 km	(0.1 mi)	0.6 km	(0.4 mi)	200 m	(600 ft)	0.7 km	(0.5 mi)	1.7 km	(1.1 mi)
1051	**117P**	Hydrogen cyanide, stabilized												
1052	**125**	Hydrogen fluoride, anhydrous	30 m	(100 ft)	0.1 km	(0.1 mi)	0.5 km	(0.3 mi)	**Refer to table 3**					
1053	**117**	Hydrogen sulfide	30 m	(100 ft)	0.1 km	(0.1 mi)	0.5 km	(0.3 mi)	400 m	(1250 ft)	2.2 km	(1.4 mi)	6.3 km	(3.9 mi)
1053	**117**	Hydrogen sulphide												
1061	**118**	Methylamine, anhydrous	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	200 m	(600 ft)	0.7 km	(0.4 mi)	2.1 km	(1.3 mi)
1062	**123**	Methyl bromide	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	150 m	(500 ft)	0.3 km	(0.2 mi)	0.8 km	(0.5 mi)
1064	**117**	Methyl mercaptan	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	200 m	(600 ft)	1.3 km	(0.8 mi)	4.1 km	(2.6 mi)
1067	**124**	Dinitrogen tetroxide	30 m	(100 ft)	0.1 km	(0.1 mi)	0.4 km	(0.3 mi)	400 m	(1250 ft)	1.4 km	(0.9 mi)	3.3 km	(2.1 mi)
1067	**124**	Nitrogen dioxide												
1069	**125**	Nitrosyl chloride	30 m	(100 ft)	0.2 km	(0.2 mi)	1.0 km	(0.6 mi)	800 m	(2500 ft)	4.3 km	(2.7 mi)	10.8 km	(6.7 mi)
1076	**125**	Phosgene	100 m	(300 ft)	0.6 km	(0.4 mi)	2.4 km	(1.5 mi)	500 m	(1500 ft)	2.9 km	(1.8 mi)	9.2 km	(5.7 mi)
1079	**125**	Sulfur dioxide	100 m	(300 ft)	0.6 km	(0.4 mi)	2.5 km	(1.6 mi)	**Refer to table 3**					
1079	**125**	Sulphur dioxide												
1082	**119P**	Refrigerant gas R-1113	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	60 m	(200 ft)	0.4 km	(0.2 mi)	0.8 km	(0.5 mi)
1082	**119P**	Trifluorochloroethylene, stabilized												
1092	**131P**	Acrolein, stabilized	100 m	(300 ft)	1.2 km	(0.8 mi)	3.3 km	(2.1 mi)	500 m	(1500 ft)	6.1 km	(3.8 mi)	10.8 km	(6.7 mi)
1093	**131P**	Acrylonitrile, stabilized	30 m	(100 ft)	0.2 km	(0.2 mi)	0.6 km	(0.4 mi)	100 m	(300 ft)	1.2 km	(0.8 mi)	2.3 km	(1.4 mi)
1098	**131**	Allyl alcohol	30 m	(100 ft)	0.2 km	(0.1 mi)	0.3 km	(0.2 mi)	60 m	(200 ft)	0.7 km	(0.5 mi)	1.2 km	(0.8 mi)
1135	**131**	Ethylene chlorohydrin	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)
1143	**131P**	Crotonaldehyde	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	60 m	(200 ft)	0.5 km	(0.3 mi)	0.7 km	(0.5 mi)
1143	**131P**	Crotonaldehyde, stabilized												

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
1162	**155**	Dimethyldichlorosilane **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.2 mi)	60 m (200 ft)	0.6 km (0.4 mi)	1.8 km (1.1 mi)
1163	**131**	Dimethylhydrazine, unsymmetrical	30 m (100 ft)	0.2 km (0.1 mi)	0.5 km (0.3 mi)	100 m (300 ft)	1.0 km (0.6 mi)	1.8 km (1.1 mi)
1182	**155**	Ethyl chloroformate	30 m (100 ft)	0.2 km (0.1 mi)	0.3 km (0.2 mi)	60 m (200 ft)	0.6 km (0.4 mi)	0.9 km (0.6 mi)
1183	**139**	Ethyldichlorosilane **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	60 m (200 ft)	0.6 km (0.4 mi)	2.0 km (1.3 mi)
1185	**131P**	Ethyleneimine, stabilized	30 m (100 ft)	0.2 km (0.1 mi)	0.5 km (0.3 mi)	200 m (600 ft)	0.9 km (0.6 mi)	1.8 km (1.1 mi)
1196	**155**	Ethyltrichlorosilane **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.5 km (0.3 mi)	200 m (600 ft)	2.1 km (1.3 mi)	5.8 km (3.6 mi)
1238	**155**	Methyl chloroformate	30 m (100 ft)	0.2 km (0.2 mi)	0.5 km (0.4 mi)	150 m (500 ft)	1.1 km (0.7 mi)	2.1 km (1.3 mi)
1239	**131**	Methyl chloromethyl ether	60 m (200 ft)	0.5 km (0.3 mi)	1.5 km (0.9 mi)	300 m (1000 ft)	3.1 km (2.0 mi)	5.8 km (3.6 mi)
1242	**139**	Methyldichlorosilane **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	60 m (200 ft)	0.8 km (0.5 mi)	2.3 km (1.5 mi)
1244	**131**	Methylhydrazine	30 m (100 ft)	0.3 km (0.2 mi)	0.6 km (0.4 mi)	100 m (300 ft)	1.4 km (0.9 mi)	2.1 km (1.3 mi)
1250	**155**	Methyltrichlorosilane **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	60 m (200 ft)	0.8 km (0.5 mi)	2.5 km (1.6 mi)
1251	**131P**	Methyl vinyl ketone, stabilized	100 m (300 ft)	0.3 km (0.2 mi)	0.7 km (0.4 mi)	800 m (2500 ft)	1.6 km (1.0 mi)	2.8 km (1.8 mi)
1259	**131**	Nickel carbonyl	100 m (300 ft)	1.3 km (0.8 mi)	5.0 km (3.1 mi)	1000 m (3000 ft)	10.8 km (6.8 mi)	11.0+ km (7.0+ mi)

1295	**139**	Trichlorosilane **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	60 m	(200 ft)	0.6 km	(0.4 mi)	2.1 km	(1.3 mi)
1298	**155**	Trimethylchlorosilane **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	60 m	(200 ft)	0.5 km	(0.3 mi)	1.4 km	(0.9 mi)
1305	**155P**	Vinyltrichlorosilane **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	60 m	(200 ft)	0.6 km	(0.4 mi)	1.9 km	(1.2 mi)
1305	**155P**	Vinyltrichlorosilane, stabilized **(when spilled in water)**												
1340	**139**	Phosphorus pentasulfide, free from yellow and white Phosphorus **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	60 m	(200 ft)	0.3 km	(0.2 mi)	1.4 km	(0.9 mi)
1340	**139**	Phosphorus pentasulphide, free from yellow and white Phosphorus **(when spilled in water)**												
1360	**139**	Calcium phosphide **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.4 km	(0.3 mi)	300 m	(1000 ft)	1.0 km	(0.6 mi)	3.5 km	(2.2 mi)
1380	**135**	Pentaborane	60 m	(200 ft)	0.6 km	(0.4 mi)	1.9 km	(1.2 mi)	200 m	(600 ft)	2.7 km	(1.7 mi)	6.2 km	(3.9 mi)
1384	**135**	Sodium dithionite **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.4 km	(0.3 mi)	60 m	(200 ft)	0.6 km	(0.4 mi)	2.5 km	(1.6 mi)
1384	**135**	Sodium hydrosulfite **(when spilled in water)**												
1384	**135**	Sodium hydrosulphite **(when spilled in water)**												
1390	**139**	Alkali metal amides **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	60 m	(200 ft)	0.6 km	(0.4 mi)	2.2 km	(1.4 mi)
1397	**139**	Aluminum phosphide **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.7 km	(0.5 mi)	500 m	(1500 ft)	2.0 km	(1.2 mi)	6.5 km	(4.0 mi)

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
1419	**139**	Magnesium aluminum phosphide **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.6 km (0.4 mi)	500 m (1500 ft)	1.8 km (1.1 mi)	5.8 km (3.6 mi)
1432	**139**	Sodium phosphide **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.4 km (0.2 mi)	300 m (1000 ft)	1.3 km (0.8 mi)	3.8 km (2.4 mi)
1510	**143**	Tetranitromethane	30 m (100 ft)	0.2 km (0.1 mi)	0.3 km (0.2 mi)	30 m (100 ft)	0.4 km (0.3 mi)	0.7 km (0.4 mi)
1541	**155**	Acetone cyanohydrin, stabilized **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	60 m (200 ft)	0.2 km (0.2 mi)	0.8 km (0.5 mi)
1556	**152**	Methyldichloroarsine	100 m (300 ft)	1.4 km (0.9 mi)	2.1 km (1.3 mi)	300 m (1000 ft)	3.8 km (2.4 mi)	5.2 km (3.3 mi)
1560	**157**	Arsenic chloride	30 m (100 ft)	0.2 km (0.1 mi)	0.3 km (0.2 mi)	100 m (300 ft)	1.0 km (0.6 mi)	1.5 km (1.0 mi)
1560	**157**	Arsenic trichloride						
1569	**131**	Bromoacetone	30 m (100 ft)	0.4 km (0.3 mi)	1.2 km (0.7 mi)	150 m (500 ft)	1.6 km (1.0 mi)	3.2 km (2.0 mi)
1580	**154**	Chloropicrin	60 m (200 ft)	0.5 km (0.3 mi)	1.2 km (0.8 mi)	200 m (600 ft)	2.2 km (1.4 mi)	3.6 km (2.3 mi)
1581	**123**	Chloropicrin and Methyl bromide mixture	30 m (100 ft)	0.1 km (0.1 mi)	0.6 km (0.4 mi)	300 m (1000 ft)	2.1 km (1.3 mi)	5.9 km (3.7 mi)
1581	**123**	Methyl bromide and Chloropicrin mixture						
1582	**119**	Chloropicrin and Methyl chloride mixture	30 m (100 ft)	0.1 km (0.1 mi)	0.4 km (0.3 mi)	60 m (200 ft)	0.4 km (0.2 mi)	1.7 km (1.1 mi)
1582	**119**	Methyl chloride and Chloropicrin mixture						
1583	**154**	Chloropicrin mixture, n.o.s.	60 m (200 ft)	0.5 km (0.3 mi)	1.2 km (0.8 mi)	200 m (600 ft)	2.2 km (1.4 mi)	3.6 km (2.3 mi)

1589	**125**	Cyanogen chloride, stabilized	300 m	(1000 ft)	1.8 km	(1.2 mi)	6.4 km	(4.0 mi)	1000 m	(3000 ft)	9.7 km	(6.0 mi)	11.0+ km	(7.0+ mi)
1595 1595	**156** **156**	Dimethyl sulfate Dimethyl sulphate	30 m	(100 ft)	0.2 km	(0.1 mi)	0.2 km	(0.1 mi)	60 m	(200 ft)	0.5 km	(0.3 mi)	0.6 km	(0.4 mi)
1605	**154**	Ethylene dibromide	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)
1612 1612	**123** **123**	Compressed gas and hexaethyl tetraphosphate mixture Hexaethyl tetraphosphate and compressed gas mixture	100 m	(300 ft)	0.8 km	(0.5 mi)	2.7 km	(1.7 mi)	400 m	(1250 ft)	3.5 km	(2.2 mi)	8.1 km	(5.1 mi)
1613 1613	**154** **154**	Hydrocyanic acid, aqueous solution, with not more than 20% Hydrogen cyanide Hydrogen cyanide, aqueous solution, with not more than 20% Hydrogen cyanide	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	100 m	(300 ft)	0.5 km	(0.3 mi)	1.1 km	(0.7 mi)
1614	**152**	Hydrogen cyanide, stabilized (absorbed)	60 m	(200 ft)	0.2 km	(0.1 mi)	0.6 km	(0.4 mi)	150 m	(500 ft)	0.5 km	(0.3 mi)	1.5 km	(0.9 mi)
1647 1647	**151** **151**	Ethylene dibromide and Methyl bromide mixture, liquid Methyl bromide and Ethylene dibromide mixture, liquid	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	150 m	(500 ft)	0.3 km	(0.2 mi)	0.8 km	(0.5 mi)
1660 1660	**124** **124**	Nitric oxide Nitric oxide, compressed	30 m	(100 ft)	0.1 km	(0.1 mi)	0.6 km	(0.4 mi)	100 m	(300 ft)	0.6 km	(0.4 mi)	2.2 km	(1.4 mi)
1670	**157**	Perchloromethyl mercaptan	30 m	(100 ft)	0.2 km	(0.2 mi)	0.4 km	(0.2 mi)	100 m	(300 ft)	0.8 km	(0.5 mi)	1.2 km	(0.8 mi)
1672	**151**	Phenylcarbylamine chloride	30 m	(100 ft)	0.2 km	(0.1 mi)	0.2 km	(0.1 mi)	60 m	(200 ft)	0.5 km	(0.3 mi)	0.7 km	(0.4 mi)
1680	**157**	Potassium cyanide, solid **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	60 m	(200 ft)	0.2 km	(0.2 mi)	1.0 km	(0.6 mi)
1689	**157**	Sodium cyanide, solid **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	100 m	(300 ft)	0.3 km	(0.2 mi)	1.2 km	(0.7 mi)

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions	SMALL SPILLS Then PROTECT persons Downwind during DAY	SMALL SPILLS Then PROTECT persons Downwind during NIGHT	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions	LARGE SPILLS Then PROTECT persons Downwind during DAY	LARGE SPILLS Then PROTECT persons Downwind during NIGHT
			Meters (Feet)	Kilometers (Miles)	Kilometers (Miles)	Meters (Feet)	Kilometers (Miles)	Kilometers (Miles)
1695	131	Chloroacetone, stabilized	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	60 m (200 ft)	0.4 km (0.3 mi)	0.6 km (0.4 mi)
1716	156	Acetyl bromide **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.3 km (0.2 mi)	0.9 km (0.6 mi)
1717	155	Acetyl chloride **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	100 m (300 ft)	0.9 km (0.6 mi)	2.6 km (1.6 mi)
1722 1722	155 155	Allyl chlorocarbonate Allyl chloroformate	100 m (300 ft)	0.3 km (0.2 mi)	0.8 km (0.5 mi)	400 m (1250 ft)	1.4 km (0.9 mi)	2.4 km (1.5 mi)
1724	155	Allyltrichlorosilane, stabilized **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	60 m (200 ft)	0.5 km (0.3 mi)	1.7 km (1.1 mi)
1725	137	Aluminum bromide, anhydrous **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)
1726	137	Aluminum chloride, anhydrous **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	60 m (200 ft)	0.5 km (0.3 mi)	2.0 km (1.2 mi)
1728	155	Amyltrichlorosilane **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	60 m (200 ft)	0.5 km (0.3 mi)	1.7 km (1.0 mi)
1732	157	Antimony pentafluoride **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)	100 m (300 ft)	1.1 km (0.7 mi)	3.9 km (2.4 mi)
1741	125	Boron trichloride **(when spilled on land)**	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)	100 m (300 ft)	0.6 km (0.4 mi)	1.4 km (0.9 mi)
1741	125	Boron trichloride **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)	100 m (300 ft)	1.2 km (0.8 mi)	3.6 km (2.2 mi)

1744 1744 1744	**154** **154** **154**	Bromine Bromine, solution Bromine, solution (Inhalation Hazard Zone A)	60 m	(200 ft)	0.8 km	(0.5 mi)	2.3 km	(1.5 mi)	300 m	(1000 ft)	3.8 km	(2.4 mi)	7.5 km	(4.7 mi)
1744	**154**	Bromine, solution (Inhalation Hazard Zone B)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.2 mi)	30 m	(100 ft)	0.3 km	(0.2 mi)	0.5 km	(0.3 mi)
1745	**144**	Bromine pentafluoride **(when spilled on land)**	100 m	(300 ft)	0.9 km	(0.5 mi)	2.5 km	(1.6 mi)	400 m	(1250 ft)	5.4 km	(3.3 mi)	10.7 km	(6.6 mi)
1745	**144**	Bromine pentafluoride **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	150 m	(500 ft)	1.2 km	(0.7 mi)	4.0 km	(2.5 mi)
1746	**144**	Bromine trifluoride **(when spilled on land)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	30 m	(100 ft)	0.3 km	(0.2 mi)	0.4 km	(0.3 mi)
1746	**144**	Bromine trifluoride **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	100 m	(300 ft)	1.0 km	(0.7 mi)	3.7 km	(2.3 mi)
1747	**155**	Butyltrichlorosilane **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	60 m	(200 ft)	0.5 km	(0.3 mi)	1.6 km	(1.0 mi)
1749	**124**	Chlorine trifluoride	60 m	(200 ft)	0.3 km	(0.2 mi)	1.1 km	(0.7 mi)	200 m	(600 ft)	1.4 km	(0.9 mi)	3.6 km	(2.3 mi)
1752	**156**	Chloroacetyl chloride **(when spilled on land)**	30 m	(100 ft)	0.3 km	(0.2 mi)	0.6 km	(0.4 mi)	100 m	(300 ft)	1.1 km	(0.7 mi)	1.9 km	(1.2 mi)
1752	**156**	Chloroacetyl chloride **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.2 km	(0.1 mi)	0.6 km	(0.4 mi)
1753	**156**	Chlorophenyltrichlorosilane **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.2 km	(0.2 mi)	0.8 km	(0.5 mi)
1754	**137**	Chlorosulfonic acid (with or without sulfur trioxide) **(when spilled on land)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.2 km	(0.2 mi)	0.3 km	(0.2 mi)

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
1754	**137**	Chlorosulfonic acid (with or without sulfur trioxide) **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	60 m (200 ft)	0.7 km (0.4 mi)	2.3 km (1.4 mi)
1754	**137**	Chlorosulphonic acid (with or without sulphur trioxide) **(when spilled on land)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.2 km (0.2 mi)	0.3 km (0.2 mi)
1754	**137**	Chlorosulphonic acid (with or without sulphur trioxide) **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	60 m (200 ft)	0.7 km (0.4 mi)	2.3 km (1.4 mi)
1758	**137**	Chromium oxychloride **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.1 km (0.1 mi)	0.5 km (0.3 mi)
1762	**156**	Cyclohexenyltrichlorosilane **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.3 km (0.2 mi)	1.2 km (0.7 mi)
1763	**156**	Cyclohexyltrichlorosilane **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.3 km (0.2 mi)	1.2 km (0.7 mi)
1765	**156**	Dichloroacetyl chloride **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.2 km (0.1 mi)	0.7 km (0.5 mi)
1766	**156**	Dichlorophenyltrichlorosilane **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	60 m (200 ft)	0.5 km (0.4 mi)	2.0 km (1.2 mi)
1767	**155**	Diethyldichlorosilane **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.3 km (0.2 mi)	0.9 km (0.5 mi)

1769	**156**	Diphenyldichlorosilane **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.3 km	(0.2 mi)	1.1 km	(0.7 mi)
1771	**156**	Dodecyltrichlorosilane **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.4 km	(0.3 mi)	1.2 km	(0.8 mi)
1777	**137**	Fluorosulfonic acid **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.2 km	(0.1 mi)	0.5 km	(0.3 mi)
1777	**137**	Fluorosulphonic acid **(when spilled in water)**												
1781	**156**	Hexadecyltrichlorosilane **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.4 km	(0.3 mi)
1784	**156**	Hexyltrichlorosilane **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.4 km	(0.2 mi)	1.3 km	(0.8 mi)
1799	**156**	Nonyltrichlorosilane **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.4 km	(0.3 mi)	1.4 km	(0.9 mi)
1800	**156**	Octadecyltrichlorosilane **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.4 km	(0.3 mi)	1.3 km	(0.8 mi)
1801	**156**	Octyltrichlorosilane **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.4 km	(0.3 mi)	1.4 km	(0.9 mi)
1804	**156**	Phenyltrichlorosilane **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.4 km	(0.2 mi)	1.3 km	(0.8 mi)
1806	**137**	Phosphorus pentachloride **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.3 km	(0.2 mi)	1.3 km	(0.8 mi)
1808	**137**	Phosphorus tribromide **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.4 km	(0.3 mi)	1.5 km	(0.9 mi)
1809	**137**	Phosphorus trichloride **(when spilled on land)**	30 m	(100 ft)	0.2 km	(0.2 mi)	0.6 km	(0.4 mi)	100 m	(300 ft)	1.0 km	(0.7 mi)	2.1 km	(1.3 mi)
1809	**137**	Phosphorus trichloride **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	60 m	(200 ft)	0.7 km	(0.4 mi)	2.4 km	(1.5 mi)

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
1810	137	Phosphorus oxychloride **(when spilled on land)**	30 m (100 ft)	0.3 km (0.2 mi)	0.6 km (0.4 mi)	100 m (300 ft)	1.0 km (0.7 mi)	1.9 km (1.2 mi)
1810	137	Phosphorus oxychloride **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	60 m (200 ft)	0.6 km (0.4 mi)	2.1 km (1.3 mi)
1815	132	Propionyl chloride **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.2 km (0.1 mi)	0.5 km (0.3 mi)
1816	155	Propyltrichlorosilane **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	60 m (200 ft)	0.5 km (0.3 mi)	1.9 km (1.2 mi)
1818	157	Silicon tetrachloride **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	60 m (200 ft)	0.8 km (0.5 mi)	2.7 km (1.7 mi)
1828	137	Sulfur chlorides **(when spilled on land)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	60 m (200 ft)	0.3 km (0.2 mi)	0.4 km (0.3 mi)
1828	137	Sulfur chlorides **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.3 km (0.2 mi)	1.0 km (0.6 mi)
1828	137	Sulphur chlorides **(when spilled on land)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	60 m (200 ft)	0.3 km (0.2 mi)	0.4 km (0.3 mi)
1828	137	Sulphur chlorides **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.3 km (0.2 mi)	1.0 km (0.6 mi)
1829	137	Sulfur trioxide, stabilized	60 m (200 ft)	0.4 km (0.2 mi)	1.0 km (0.6 mi)	300 m (1000 ft)	2.9 km (1.8 mi)	6.3 km (4.0 mi)
1829	137	Sulphur trioxide, stabilized						
1831	137	Sulfuric acid, fuming	60 m (200 ft)	0.4 km (0.2 mi)	1.0 km (0.6 mi)	300 m (1000 ft)	2.9 km (1.8 mi)	6.3 km (4.0 mi)
1831	137	Sulphuric acid, fuming						

1834	**137**	Sulfuryl chloride **(when spilled on land)**	30 m	(100 ft)	0.2 km	(0.1 mi)	0.4 km	(0.3 mi)	60 m	(200 ft)	0.8 km	(0.5 mi)	1.5 km	(0.9 mi)
1834	**137**	Sulfuryl chloride **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.4 km	(0.3 mi)	1.6 km	(1.0 mi)
1834	**137**	Sulphuryl chloride **(when spilled on land)**	30 m	(100 ft)	0.2 km	(0.1 mi)	0.4 km	(0.3 mi)	60 m	(200 ft)	0.8 km	(0.5 mi)	1.5 km	(0.9 mi)
1834	**137**	Sulphuryl chloride **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.4 km	(0.3 mi)	1.6 km	(1.0 mi)
1836	**137**	Thionyl chloride **(when spilled on land)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.2 mi)	30 m	(100 ft)	0.3 km	(0.2 mi)	0.5 km	(0.3 mi)
1836	**137**	Thionyl chloride **(when spilled in water)**	100 m	(300 ft)	0.9 km	(0.6 mi)	2.9 km	(1.8 mi)	800 m	(2500 ft)	9.7 km	(6.0 mi)	11.0+ km	(7.0+ mi)
1838	**137**	Titanium tetrachloride **(when spilled on land)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	30 m	(100 ft)	0.3 km	(0.2 mi)	0.5 km	(0.3 mi)
1838	**137**	Titanium tetrachloride **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	60 m	(200 ft)	0.5 km	(0.3 mi)	1.7 km	(1.0 mi)
1859 1859	**125** **125**	Silicon tetrafluoride Silicon tetrafluoride, compressed	30 m	(100 ft)	0.2 km	(0.1 mi)	0.8 km	(0.5 mi)	100 m	(300 ft)	0.5 km	(0.3 mi)	1.8 km	(1.2 mi)
1892	**151**	Ethyldichloroarsine	150 m	(500 ft)	1.5 km	(0.9 mi)	2.1 km	(1.3 mi)	400 m	(1250 ft)	4.6 km	(2.9 mi)	6.4 km	(4.0 mi)
1898	**156**	Acetyl iodide **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.4 km	(0.3 mi)	1.1 km	(0.7 mi)
1911 1911 1911	**119** **119** **119**	Diborane Diborane, compressed Diborane mixtures	60 m	(200 ft)	0.3 km	(0.2 mi)	1.2 km	(0.7 mi)	300 m	(1000 ft)	1.5 km	(1.0 mi)	4.6 km	(2.9 mi)

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
1923	**135**	Calcium dithionite **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.4 km (0.3 mi)	60 m (200 ft)	0.7 km (0.4 mi)	2.6 km (1.6 mi)
1923	**135**	Calcium hydrosulfite **(when spilled in water)**						
1923	**135**	Calcium hydrosulphite **(when spilled in water)**						
1929	**135**	Potassium dithionite **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.4 km (0.2 mi)	60 m (200 ft)	0.6 km (0.4 mi)	2.3 km (1.5 mi)
1929	**135**	Potassium hydrosulfite **(when spilled in water)**						
1929	**135**	Potassium hydrosulphite **(when spilled in water)**						
1931	**171**	Zinc dithionite **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.4 km (0.3 mi)	60 m (200 ft)	0.6 km (0.4 mi)	2.4 km (1.5 mi)
1931	**171**	Zinc hydrosulfite **(when spilled in water)**						
1931	**171**	Zinc hydrosulphite **(when spilled in water)**						
1953	**119**	Compressed gas, poisonous, flammable, n.o.s.	150 m (500 ft)	1.0 km (0.6 mi)	3.8 km (2.4 mi)	1000 m (3000 ft)	5.7 km (3.6 mi)	10.1 km (6.3 mi)
1953	**119**	Compressed gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone A)						
1953	**119**	Compressed gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone B)	30 m (100 ft)	0.1 km (0.1 mi)	0.4 km (0.2 mi)	300 m (1000 ft)	1.3 km (0.8 mi)	3.4 km (2.1 mi)

1953	**119**	Compressed gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	150 m	(500 ft)	1.0 km	(0.6 mi)	2.9 km	(1.8 mi)
1953	**119**	Compressed gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone D)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	150 m	(500 ft)	0.8 km	(0.5 mi)	2.0 km	(1.3 mi)
1953	**119**	Compressed gas, toxic, flammable, n.o.s.												
1953	**119**	Compressed gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone A)	150 m	(500 ft)	1.0 km	(0.6 mi)	3.8 km	(2.4 mi)	1000 m	(3000 ft)	5.7 km	(3.6 mi)	10.1 km	(6.3 mi)
1953	**119**	Compressed gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone B)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.4 km	(0.2 mi)	300 m	(1000 ft)	1.3 km	(0.8 mi)	3.4 km	(2.1 mi)
1953	**119**	Compressed gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	150 m	(500 ft)	1.0 km	(0.6 mi)	2.9 km	(1.8 mi)
1953	**119**	Compressed gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone D)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	150 m	(500 ft)	0.8 km	(0.5 mi)	2.0 km	(1.3 mi)
1955	**123**	Compressed gas, poisonous, n.o.s.												
1955	**123**	Compressed gas, poisonous, n.o.s. (Inhalation Hazard Zone A)	100 m	(300 ft)	0.5 km	(0.3 mi)	2.5 km	(1.6 mi)	1000 m	(3000 ft)	5.7 km	(3.6 mi)	10.1 km	(6.3 mi)
1955	**123**	Compressed gas, poisonous, n.o.s. (Inhalation Hazard Zone B)	30 m	(100 ft)	0.2 km	(0.1 mi)	0.9 km	(0.6 mi)	400 m	(1250 ft)	2.3 km	(1.4 mi)	5.1 km	(3.2 mi)
1955	**123**	Compressed gas, poisonous, n.o.s. (Inhalation Hazard Zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	150 m	(500 ft)	1.0 km	(0.6 mi)	2.9 km	(1.8 mi)

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
1955	123	Compressed gas, poisonous, n.o.s. (Inhalation Hazard Zone D)	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	150 m (500 ft)	0.8 km (0.5 mi)	2.0 km (1.3 mi)
1955	123	Compressed gas, toxic, n.o.s.						
1955	123	Compressed gas, toxic, n.o.s. (Inhalation Hazard Zone A)	100 m (300 ft)	0.5 km (0.3 mi)	2.5 km (1.6 mi)	1000 m (3000 ft)	5.7 km (3.6 mi)	10.1 km (6.3 mi)
1955	123	Compressed gas, toxic, n.o.s. (Inhalation Hazard Zone B)	30 m (100 ft)	0.2 km (0.1 mi)	0.9 km (0.6 mi)	400 m (1250 ft)	2.3 km (1.4 mi)	5.1 km (3.2 mi)
1955	123	Compressed gas, toxic, n.o.s. (Inhalation Hazard Zone C)	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)	150 m (500 ft)	1.0 km (0.6 mi)	2.9 km (1.8 mi)
1955	123	Compressed gas, toxic, n.o.s. (Inhalation Hazard Zone D)	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	150 m (500 ft)	0.8 km (0.5 mi)	2.0 km (1.3 mi)
1955	123	Organic phosphate compound mixed with compressed gas						
1955	123	Organic phosphate mixed with compressed gas	100 m (300 ft)	1.0 km (0.7 mi)	3.4 km (2.1 mi)	500 m (1500 ft)	4.4 km (2.7 mi)	9.6 km (6.0 mi)
1955	123	Organic phosphorus compound mixed with compressed gas						
1967	123	Insecticide gas, poisonous, n.o.s.						
1967	123	Insecticide gas, toxic, n.o.s.	100 m (300 ft)	1.0 km (0.7 mi)	3.4 km (2.1 mi)	500 m (1500 ft)	4.4 km (2.7 mi)	9.6 km (6.0 mi)
1967	123	Parathion and compressed gas mixture						

1975	**124**	Dinitrogen tetroxide and Nitric oxide mixture	30 m	(100 ft)	0.1 km	(0.1 mi)	0.6 km	(0.4 mi)	100 m	(300 ft)	0.6 km	(0.4 mi)	2.2 km	(1.4 mi)
1975	**124**	Nitric oxide and Dinitrogen tetroxide mixture												
1975	**124**	Nitric oxide and Nitrogen dioxide mixture												
1975	**124**	Nitrogen dioxide and Nitric oxide mixture												
1994	**136**	Iron pentacarbonyl	100 m	(300 ft)	0.9 km	(0.6 mi)	2.0 km	(1.2 mi)	400 m	(1250 ft)	4.8 km	(3.0 mi)	7.5 km	(4.7 mi)
2004	**135**	Magnesium diamide **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	60 m	(200 ft)	0.6 km	(0.4 mi)	2.2 km	(1.4 mi)
2011	**139**	Magnesium phosphide **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.6 km	(0.4 mi)	500 m	(1500 ft)	1.7 km	(1.1 mi)	5.4 km	(3.4 mi)
2012	**139**	Potassium phosphide **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	300 m	(1000 ft)	1.1 km	(0.7 mi)	3.6 km	(2.2 mi)
2013	**139**	Strontium phosphide **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	300 m	(1000 ft)	1.1 km	(0.7 mi)	3.4 km	(2.2 mi)
2032	**157**	Nitric acid, red fuming	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	150 m	(500 ft)	0.3 km	(0.2 mi)	0.5 km	(0.3 mi)
2186	**125**	Hydrogen chloride, refrigerated liquid	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	**Refer to table 3**					
2188	**119**	Arsine	150 m	(500 ft)	1.0 km	(0.6 mi)	3.8 km	(2.4 mi)	1000 m	(3000 ft)	5.7 km	(3.6 mi)	10.1 km	(6.3 mi)
2189	**119**	Dichlorosilane	30 m	(100 ft)	0.1 km	(0.1 mi)	0.4 km	(0.2 mi)	300 m	(1000 ft)	1.3 km	(0.8 mi)	3.4 km	(2.1 mi)
2190	**124**	Oxygen difluoride	300 m	(1000 ft)	1.8 km	(1.1 mi)	7.1 km	(4.4 mi)	1000 m	(3000 ft)	11.0+ km	(7.0+ mi)	11.0+ km	(7.0+ mi)
2190	**124**	Oxygen difluoride, compressed												
2191	**123**	Sulfuryl fluoride	30 m	(100 ft)	0.1 km	(0.1 mi)	0.5 km	(0.3 mi)	400 m	(1250 ft)	2.2 km	(1.4 mi)	5.3 km	(3.3 mi)
2191	**123**	Sulphuryl fluoride												
2192	**119**	Germane	150 m	(500 ft)	0.9 km	(0.5 mi)	3.3 km	(2.1 mi)	500 m	(1500 ft)	3.3 km	(2.1 mi)	7.5 km	(4.7 mi)
2194	**125**	Selenium hexafluoride	200 m	(600 ft)	1.1 km	(0.7 mi)	3.5 km	(2.2 mi)	600 m	(2000 ft)	3.5 km	(2.2 mi)	7.9 km	(4.9 mi)

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
2195	**125**	Tellurium hexafluoride	1000 m (3000 ft)	5.8 km (3.6 mi)	10.9 km (6.8 mi)	1000 m (3000 ft)	11.0+ km (7.0+ mi)	11.0+ km (7.0+ mi)
2196	**125**	Tungsten hexafluoride	30 m (100 ft)	0.2 km (0.1 mi)	0.8 km (0.5 mi)	150 m (500 ft)	0.8 km (0.5 mi)	2.7 km (1.7 mi)
2197	**125**	Hydrogen iodide, anhydrous	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)	150 m (500 ft)	1.0 km (0.6 mi)	2.9 km (1.8 mi)
2198	**125**	Phosphorus pentafluoride	30 m (100 ft)	0.2 km (0.2 mi)	1.0 km (0.7 mi)	150 m (500 ft)	1.0 km (0.6 mi)	3.5 km (2.2 mi)
2198	**125**	Phosphorus pentafluoride, compressed						
2199	**119**	Phosphine	60 m (200 ft)	0.3 km (0.2 mi)	1.1 km (0.7 mi)	300 m (1000 ft)	1.3 km (0.8 mi)	3.7 km (2.3 mi)
2202	**117**	Hydrogen selenide, anhydrous	300 m (1000 ft)	1.7 km (1.1 mi)	6.0 km (3.7 mi)	1000 m (3000 ft)	10.7 km (6.7 mi)	11.0+ km (7.0+ mi)
2204	**119**	Carbonyl sulfide	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)	300 m (1000 ft)	1.6 km (1.0 mi)	3.8 km (2.4 mi)
2204	**119**	Carbonyl sulphide						
2232	**153**	Chloroacetaldehyde	30 m (100 ft)	0.2 km (0.1 mi)	0.3 km (0.2 mi)	60 m (200 ft)	0.6 km (0.4 mi)	1.1 km (0.7 mi)
2232	**153**	2-Chloroethanal						
2285	**156**	Isocyanatobenzotrifluorides	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	30 m (100 ft)	0.4 km (0.3 mi)	0.6 km (0.4 mi)
2308	**157**	Nitrosylsulfuric acid, liquid **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)	300 m (1000 ft)	1.0 km (0.6 mi)	2.9 km (1.8 mi)
2308	**157**	Nitrosylsulphuric acid, liquid **(when spilled in water)**						
2334	**131**	Allylamine	30 m (100 ft)	0.2 km (0.1 mi)	0.5 km (0.4 mi)	150 m (500 ft)	1.4 km (0.9 mi)	2.5 km (1.6 mi)
2337	**131**	Phenyl mercaptan	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.3 km (0.2 mi)	0.4 km (0.2 mi)
2353	**132**	Butyryl chloride **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.3 km (0.2 mi)	0.7 km (0.5 mi)

2382	**131**	Dimethylhydrazine, symmetrical	30 m	(100 ft)	0.2 km	(0.1 mi)	0.3 km	(0.2 mi)	60 m	(200 ft)	0.7 km	(0.5 mi)	1.3 km	(0.8 mi)
2395	**132**	Isobutyryl chloride **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.2 km	(0.1 mi)	0.4 km	(0.3 mi)
2407	**155**	Isopropyl chloroformate	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.2 mi)	60 m	(200 ft)	0.5 km	(0.3 mi)	0.9 km	(0.6 mi)
2417 2417	**125** **125**	Carbonyl fluoride Carbonyl fluoride, compressed	150 m	(500 ft)	0.7 km	(0.5 mi)	2.5 km	(1.6 mi)	600 m	(2000 ft)	3.6 km	(2.3 mi)	7.8 km	(4.9 mi)
2418 2418	**125** **125**	Sulfur tetrafluoride Sulphur tetrafluoride	100 m	(300 ft)	0.5 km	(0.3 mi)	2.3 km	(1.5 mi)	400 m	(1250 ft)	2.1 km	(1.3 mi)	6.0 km	(3.7 mi)
2420	**125**	Hexafluoroacetone	100 m	(300 ft)	0.7 km	(0.4 mi)	2.7 km	(1.7 mi)	1000 m	(3000 ft)	11.0+ km	(7.0+ mi)	11.0+ km	(7.0+ mi)
2421	**124**	Nitrogen trioxide	60 m	(200 ft)	0.3 km	(0.2 mi)	1.2 km	(0.7 mi)	200 m	(600 ft)	1.2 km	(0.8 mi)	4.2 km	(2.6 mi)
2434	**156**	Dibenzyldichlorosilane **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.4 km	(0.3 mi)
2435	**156**	Ethylphenyldichlorosilane **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.3 km	(0.2 mi)	0.9 km	(0.6 mi)
2437	**156**	Methylphenyldichlorosilane **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.4 km	(0.2 mi)	1.2 km	(0.8 mi)
2438	**131**	Trimethylacetyl chloride	60 m	(200 ft)	0.5 km	(0.3 mi)	1.0 km	(0.6 mi)	200 m	(600 ft)	2.1 km	(1.3 mi)	3.3 km	(2.1 mi)
2442	**156**	Trichloroacetyl chloride	30 m	(100 ft)	0.2 km	(0.1 mi)	0.3 km	(0.2 mi)	60 m	(200 ft)	0.7 km	(0.4 mi)	1.1 km	(0.7 mi)
2474	**157**	Thiophosgene	60 m	(200 ft)	0.6 km	(0.4 mi)	1.7 km	(1.1 mi)	200 m	(600 ft)	2.1 km	(1.3 mi)	4.0 km	(2.5 mi)
2477	**131**	Methyl isothiocyanate	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.3 km	(0.2 mi)	0.4 km	(0.3 mi)

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
2478	**155**	Isocyanate solution, flammable, poisonous, n.o.s.	60 m (200 ft)	0.8 km (0.5 mi)	1.8 km (1.1 mi)	400 m (1250 ft)	4.4 km (2.7 mi)	7.0 km (4.3 mi)
2478	**155**	Isocyanate solution, flammable, toxic, n.o.s.						
2478	**155**	Isocyanates, flammable, poisonous, n.o.s.						
2478	**155**	Isocyanates, flammable, toxic, n.o.s.						
2480	**155P**	Methyl isocyanate	150 m (500 ft)	1.7 km (1.1 mi)	5.0 km (3.1 mi)	1000 m (3000 ft)	11.0+ km (7.0+ mi)	11.0+ km (7.0+ mi)
2481	**155**	Ethyl isocyanate	150 m (500 ft)	2.0 km (1.2 mi)	5.1 km (3.2 mi)	1000 m (3000 ft)	11.0+ km (7.0+ mi)	11.0+ km (7.0+ mi)
2482	**155P**	n-Propyl isocyanate	100 m (300 ft)	1.3 km (0.8 mi)	2.7 km (1.7 mi)	600 m (2000 ft)	7.4 km (4.6 mi)	10.8 km (6.7 mi)
2483	**155P**	Isopropyl isocyanate	150 m (500 ft)	1.5 km (0.9 mi)	3.2 km (2.0 mi)	1000 m (3000 ft)	11.0 km (6.9 mi)	11.0+ km (7.0+ mi)
2484	**155**	tert-Butyl isocyanate	60 m (200 ft)	0.8 km (0.5 mi)	1.8 km (1.1 mi)	400 m (1250 ft)	4.4 km (2.7 mi)	7.0 km (4.3 mi)
2485	**155P**	n-Butyl isocyanate	60 m (200 ft)	0.6 km (0.4 mi)	1.1 km (0.7 mi)	200 m (600 ft)	2.6 km (1.7 mi)	4.0 km (2.5 mi)
2486	**155P**	Isobutyl isocyanate	60 m (200 ft)	0.6 km (0.4 mi)	1.2 km (0.8 mi)	300 m (1000 ft)	3.1 km (1.9 mi)	4.7 km (3.0 mi)
2487	**155**	Phenyl isocyanate	100 m (300 ft)	0.9 km (0.6 mi)	1.4 km (0.9 mi)	300 m (1000 ft)	3.7 km (2.3 mi)	5.4 km (3.4 mi)
2488	**155**	Cyclohexyl isocyanate	30 m (100 ft)	0.3 km (0.2 mi)	0.4 km (0.3 mi)	100 m (300 ft)	1.0 km (0.6 mi)	1.4 km (0.9 mi)
2495	**144**	Iodine pentafluoride **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)	100 m (300 ft)	1.1 km (0.7 mi)	4.1 km (2.6 mi)
2521	**131P**	Diketene, stabilized	30 m (100 ft)	0.2 km (0.1 mi)	0.3 km (0.2 mi)	60 m (200 ft)	0.6 km (0.4 mi)	1.0 km (0.6 mi)
2534	**119**	Methylchlorosilane	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)	150 m (500 ft)	0.7 km (0.5 mi)	1.9 km (1.2 mi)

2548	**124**	Chlorine pentafluoride	100 m	(300 ft)	0.5 km	(0.3 mi)	2.5 km	(1.6 mi)	800 m	(2500 ft)	5.0 km	(3.1 mi)	11.0+ km	(7.0+ mi)
2605	**155**	Methoxymethyl isocyanate	30 m	(100 ft)	0.2 km	(0.1 mi)	0.2 km	(0.2 mi)	60 m	(200 ft)	0.6 km	(0.4 mi)	0.9 km	(0.6 mi)
2606	**155**	Methyl orthosilicate	30 m	(100 ft)	0.2 km	(0.1 mi)	0.3 km	(0.2 mi)	60 m	(200 ft)	0.7 km	(0.4 mi)	1.1 km	(0.7 mi)
2644	**151**	Methyl iodide	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	100 m	(300 ft)	0.3 km	(0.2 mi)	0.7 km	(0.4 mi)
2646	**151**	Hexachlorocyclopentadiene	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.3 km	(0.2 mi)	0.3 km	(0.2 mi)
2668	**131**	Chloroacetonitrile	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.3 km	(0.2 mi)	0.4 km	(0.2 mi)
2676	**119**	Stibine	60 m	(200 ft)	0.3 km	(0.2 mi)	1.6 km	(1.0 mi)	200 m	(600 ft)	1.3 km	(0.8 mi)	4.1 km	(2.6 mi)
2691	**137**	Phosphorus pentabromide **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.5 km	(0.3 mi)
2692	**157**	Boron tribromide **(when spilled on land)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	30 m	(100 ft)	0.2 km	(0.1 mi)	0.4 km	(0.3 mi)
2692	**157**	Boron tribromide **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	60 m	(200 ft)	0.5 km	(0.3 mi)	1.9 km	(1.2 mi)
2740	**155**	n-Propyl chloroformate	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	60 m	(200 ft)	0.6 km	(0.4 mi)	1.0 km	(0.7 mi)
2742	**155**	sec-Butyl chloroformate	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	30 m	(100 ft)	0.4 km	(0.2 mi)	0.5 km	(0.3 mi)
2742	**155**	Chloroformates, poisonous, corrosive, flammable, n.o.s.	30 m	(100 ft)	0.2 km	(0.1 mi)	0.2 km	(0.2 mi)	60 m	(200 ft)	0.5 km	(0.3 mi)	0.7 km	(0.5 mi)
2742	**155**	Chloroformates, toxic, corrosive, flammable, n.o.s.												
2742	**155**	Isobutyl chloroformate	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.3 km	(0.2 mi)	0.5 km	(0.3 mi)
2743	**155**	n-Butyl chloroformate	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.3 km	(0.2 mi)	0.4 km	(0.3 mi)
2806	**139**	Lithium nitride **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.2 mi)	60 m	(200 ft)	0.5 km	(0.3 mi)	1.9 km	(1.2 mi)
2826	**155**	Ethyl chlorothioformate	30 m	(100 ft)	0.2 km	(0.1 mi)	0.2 km	(0.2 mi)	60 m	(200 ft)	0.5 km	(0.3 mi)	0.7 km	(0.5 mi)
2845	**135**	Ethyl phosphonous dichloride, anhydrous	30 m	(100 ft)	0.3 km	(0.2 mi)	0.7 km	(0.5 mi)	100 m	(300 ft)	1.3 km	(0.8 mi)	2.3 km	(1.5 mi)

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
2845	**135**	Methyl phosphonous dichloride	30 m (100 ft)	0.4 km (0.3 mi)	1.1 km (0.7 mi)	200 m (600 ft)	2.4 km (1.5 mi)	4.1 km (2.6 mi)
2901	**124**	Bromine chloride	100 m (300 ft)	0.5 km (0.3 mi)	1.8 km (1.1 mi)	1000 m (3000 ft)	5.4 km (3.4 mi)	11.0+ km (7.0+ mi)
2927	**154**	Ethyl phosphonothioic dichloride, anhydrous	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.2 km (0.1 mi)	0.2 km (0.1 mi)
2927	**154**	Ethyl phosphorodichloridate	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.3 km (0.2 mi)	0.3 km (0.2 mi)
2965	**139**	Boron trifluoride dimethyl etherate **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)	100 m (300 ft)	1.2 km (0.8 mi)	3.6 km (2.2 mi)
2977	**166**	Radioactive material, Uranium hexafluoride, fissile **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	60 m (200 ft)	0.4 km (0.3 mi)	2.1 km (1.3 mi)
2977	**166**	Uranium hexafluoride, radioactive material, fissile **(when spilled in water)**						
2978	**166**	Radioactive material, Uranium hexafluoride, non fissile or fissile-excepted **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	60 m (200 ft)	0.4 km (0.3 mi)	2.1 km (1.3 mi)
2978	**166**	Uranium hexafluoride, radioactive material, non fissile or fissile-excepted **(when spilled in water)**						

2985	**155**	Chlorosilanes, flammable, corrosive, n.o.s. **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	60 m	(200 ft)	0.5 km	(0.3 mi)	1.6 km	(1.0 mi)
2986	**155**	Chlorosilanes, corrosive, flammable, n.o.s. **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	60 m	(200 ft)	0.5 km	(0.3 mi)	1.6 km	(1.0 mi)
2987	**156**	Chlorosilanes, corrosive, n.o.s. **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	60 m	(200 ft)	0.5 km	(0.3 mi)	1.6 km	(1.0 mi)
2988	**139**	Chlorosilanes, water-reactive, flammable, corrosive, n.o.s. **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	60 m	(200 ft)	0.5 km	(0.3 mi)	1.6 km	(1.0 mi)
3023	**131**	2-Methyl-2-heptanethiol	30 m	(100 ft)	0.2 km	(0.1 mi)	0.2 km	(0.1 mi)	60 m	(200 ft)	0.5 km	(0.4 mi)	0.8 km	(0.5 mi)
3048	**157**	Aluminum phosphide pesticide **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.7 km	(0.5 mi)	500 m	(1500 ft)	2.0 km	(1.3 mi)	6.5 km	(4.1 mi)
3057	**125**	Trifluoroacetyl chloride	30 m	(100 ft)	0.2 km	(0.1 mi)	0.9 km	(0.6 mi)	800 m	(2500 ft)	5.2 km	(3.3 mi)	11.0+ km	(7.0+ mi)
3079	**131P**	Methacrylonitrile, stabilized	30 m	(100 ft)	0.3 km	(0.2 mi)	0.7 km	(0.5 mi)	150 m	(500 ft)	1.6 km	(1.0 mi)	2.7 km	(1.7 mi)
3083	**124**	Perchloryl fluoride	30 m	(100 ft)	0.2 km	(0.2 mi)	1.1 km	(0.7 mi)	1000 m	(3000 ft)	5.5 km	(3.4 mi)	11.0+ km	(7.0+ mi)
3160	**119**	Liquefied gas, poisonous, flammable, n.o.s.												
3160	**119**	Liquefied gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone A)	150 m	(500 ft)	1.0 km	(0.6 mi)	3.8 km	(2.4 mi)	1000 m	(3000 ft)	5.7 km	(3.6 mi)	10.1 km	(6.3 mi)
3160	**119**	Liquefied gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone B)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.4 km	(0.2 mi)	300 m	(1000 ft)	1.3 km	(0.8 mi)	3.4 km	(2.1 mi)
3160	**119**	Liquefied gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	150 m	(500 ft)	1.0 km	(0.6 mi)	2.9 km	(1.8 mi)

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
3160	**119**	Liquefied gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone D)	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	150 m (500 ft)	0.8 km (0.5 mi)	2.0 km (1.3 mi)
3160	**119**	Liquefied gas, toxic, flammable, n.o.s.						
3160	**119**	Liquefied gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone A)	150 m (500 ft)	1.0 km (0.6 mi)	3.8 km (2.4 mi)	1000 m (3000 ft)	5.7 km (3.6 mi)	10.1 km (6.3 mi)
3160	**119**	Liquefied gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone B)	30 m (100 ft)	0.1 km (0.1 mi)	0.4 km (0.2 mi)	300 m (1000 ft)	1.3 km (0.8 mi)	3.4 km (2.1 mi)
3160	**119**	Liquefied gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone C)	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)	150 m (500 ft)	1.0 km (0.6 mi)	2.9 km (1.8 mi)
3160	**119**	Liquefied gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone D)	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	150 m (500 ft)	0.8 km (0.5 mi)	2.0 km (1.3 mi)
3162	**123**	Liquefied gas, poisonous, n.o.s.						
3162	**123**	Liquefied gas, poisonous, n.o.s. (Inhalation Hazard Zone A)	100 m (300 ft)	0.5 km (0.3 mi)	2.5 km (1.6 mi)	1000 m (3000 ft)	5.7 km (3.6 mi)	10.1 km (6.3 mi)
3162	**123**	Liquefied gas, poisonous, n.o.s. (Inhalation Hazard Zone B)	30 m (100 ft)	0.2 km (0.1 mi)	0.9 km (0.6 mi)	400 m (1250 ft)	2.3 km (1.4 mi)	5.1 km (3.2 mi)
3162	**123**	Liquefied gas, poisonous, n.o.s. (Inhalation Hazard Zone C)	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)	150 m (500 ft)	1.0 km (0.6 mi)	2.9 km (1.8 mi)

3162	**123**	Liquefied gas, poisonous, n.o.s. (Inhalation Hazard Zone D)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	150 m	(500 ft)	0.8 km	(0.5 mi)	2.0 km	(1.3 mi)
3162	**123**	Liquefied gas, toxic, n.o.s.	100 m	(300 ft)	0.5 km	(0.3 mi)	2.5 km	(1.6 mi)	1000 m	(3000 ft)	5.7 km	(3.6 mi)	10.1 km	(6.3 mi)
3162	**123**	Liquefied gas, toxic, n.o.s. (Inhalation Hazard Zone A)												
3162	**123**	Liquefied gas, toxic, n.o.s. (Inhalation Hazard Zone B)	30 m	(100 ft)	0.2 km	(0.1 mi)	0.9 km	(0.6 mi)	400 m	(1250 ft)	2.3 km	(1.4 mi)	5.1 km	(3.2 mi)
3162	**123**	Liquefied gas, toxic, n.o.s. (Inhalation Hazard Zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	150 m	(500 ft)	1.0 km	(0.6 mi)	2.9 km	(1.8 mi)
3162	**123**	Liquefied gas, toxic, n.o.s. (Inhalation Hazard Zone D)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	150 m	(500 ft)	0.8 km	(0.5 mi)	2.0 km	(1.3 mi)
3246	**156**	Methanesulfonyl chloride	30 m	(100 ft)	0.2 km	(0.2 mi)	0.3 km	(0.2 mi)	60 m	(200 ft)	0.7 km	(0.4 mi)	0.9 km	(0.6 mi)
3246	**156**	Methanesulphonyl chloride												
3275	**131**	Nitriles, poisonous, flammable, n.o.s.	30 m	(100 ft)	0.3 km	(0.2 mi)	0.7 km	(0.5 mi)	150 m	(500 ft)	1.6 km	(1.0 mi)	2.7 km	(1.7 mi)
3275	**131**	Nitriles, toxic, flammable, n.o.s.												
3276	**151**	Nitriles, liquid, poisonous, n.o.s.	30 m	(100 ft)	0.3 km	(0.2 mi)	0.7 km	(0.5 mi)	150 m	(500 ft)	1.6 km	(1.0 mi)	2.7 km	(1.7 mi)
3276	**151**	Nitriles, liquid, toxic, n.o.s.												
3276	**151**	Nitriles, poisonous, liquid, n.o.s.												
3276	**151**	Nitriles, toxic, liquid, n.o.s.												
3278	**151**	Organophosphorus compound, liquid, poisonous, n.o.s.	30 m	(100 ft)	0.4 km	(0.3 mi)	1.1 km	(0.7 mi)	200 m	(600 ft)	2.4 km	(1.5 mi)	4.1 km	(2.6 mi)
3278	**151**	Organophosphorus compound, liquid, toxic, n.o.s.												
3278	**151**	Organophosphorus compound, poisonous, liquid, n.o.s.												
3278	**151**	Organophosphorus compound, toxic, liquid, n.o.s.												

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
3279	**131**	Organophosphorus compound, poisonous, flammable, n.o.s.	30 m (100 ft)	0.4 km (0.3 mi)	1.1 km (0.7 mi)	200 m (600 ft)	2.4 km (1.5 mi)	4.1 km (2.6 mi)
3279	**131**	Organophosphorus compound, toxic, flammable, n.o.s.						
3280	**151**	Organoarsenic compound, liquid, n.o.s.	30 m (100 ft)	0.2 km (0.1 mi)	0.7 km (0.4 mi)	150 m (500 ft)	1.6 km (1.0 mi)	3.6 km (2.2 mi)
3281	**151**	Metal carbonyls, liquid, n.o.s.	100 m (300 ft)	1.3 km (0.8 mi)	5.0 km (3.1 mi)	1000 m (3000 ft)	10.8 km (6.8 mi)	11.0+ km (7.0+ mi)
3294	**131**	Hydrogen cyanide, solution in alcohol, with not more than 45% Hydrogen cyanide	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)	200 m (600 ft)	0.5 km (0.3 mi)	1.9 km (1.2 mi)
3300	**119P**	Carbon dioxide and Ethylene oxide mixture, with more than 87% Ethylene oxide	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.2 mi)	150 m (500 ft)	0.8 km (0.5 mi)	2.2 km (1.4 mi)
3300	**119P**	Ethylene oxide and Carbon dioxide mixture, with more than 87% Ethylene oxide						
3303	**124**	Compressed gas, poisonous, oxidizing, n.o.s.	100 m (300 ft)	0.5 km (0.3 mi)	2.5 km (1.6 mi)	800 m (2500 ft)	5.0 km (3.1 mi)	11.0+ km (7.0+ mi)
3303	**124**	Compressed gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone A)						
3303	**124**	Compressed gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone B)	60 m (200 ft)	0.3 km (0.2 mi)	1.1 km (0.7 mi)	400 m (1250 ft)	2.5 km (1.5 mi)	6.7 km (4.2 mi)

3303	**124**	Compressed gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	150 m	(500 ft)	1.0 km	(0.6 mi)	2.9 km	(1.8 mi)
3303	**124**	Compressed gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone D)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	150 m	(500 ft)	0.8 km	(0.5 mi)	2.0 km	(1.3 mi)
3303	**124**	Compressed gas, toxic, oxidizing, n.o.s.												
3303	**124**	Compressed gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone A)	100 m	(300 ft)	0.5 km	(0.3 mi)	2.5 km	(1.6 mi)	800 m	(2500 ft)	5.0 km	(3.1 mi)	11.0+ km	(7.0+ mi)
3303	**124**	Compressed gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone B)	60 m	(200 ft)	0.3 km	(0.2 mi)	1.1 km	(0.7 mi)	400 m	(1250 ft)	2.5 km	(1.5 mi)	6.7 km	(4.2 mi)
3303	**124**	Compressed gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	150 m	(500 ft)	1.0 km	(0.6 mi)	2.9 km	(1.8 mi)
3303	**124**	Compressed gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone D)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	150 m	(500 ft)	0.8 km	(0.5 mi)	2.0 km	(1.3 mi)
3304	**125**	Compressed gas, poisonous, corrosive, n.o.s.												
3304	**125**	Compressed gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone A)	100 m	(300 ft)	0.5 km	(0.3 mi)	2.5 km	(1.6 mi)	500 m	(1500 ft)	2.9 km	(1.8 mi)	9.2 km	(5.7 mi)
3304	**125**	Compressed gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone B)	30 m	(100 ft)	0.2 km	(0.2 mi)	1.0 km	(0.7 mi)	400 m	(1250 ft)	2.3 km	(1.4 mi)	5.1 km	(3.2 mi)
3304	**125**	Compressed gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.5 km	(0.3 mi)	300 m	(1000 ft)	1.6 km	(1.0 mi)	3.2 km	(2.0 mi)

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
3304	**125**	Compressed gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone D)	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	150 m (500 ft)	0.8 km (0.5 mi)	2.0 km (1.3 mi)
3304	**125**	Compressed gas, toxic, corrosive, n.o.s.	100 m (300 ft)	0.5 km (0.3 mi)	2.5 km (1.6 mi)	500 m (1500 ft)	2.9 km (1.8 mi)	9.2 km (5.7 mi)
3304	**125**	Compressed gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone A)						
3304	**125**	Compressed gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone B)	30 m (100 ft)	0.2 km (0.2 mi)	1.0 km (0.7 mi)	400 m (1250 ft)	2.3 km (1.4 mi)	5.1 km (3.2 mi)
3304	**125**	Compressed gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone C)	30 m (100 ft)	0.1 km (0.1 mi)	0.5 km (0.3 mi)	300 m (1000 ft)	1.6 km (1.0 mi)	3.2 km (2.0 mi)
3304	**125**	Compressed gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone D)	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	150 m (500 ft)	0.8 km (0.5 mi)	2.0 km (1.3 mi)
3305	**119**	Compressed gas, poisonous, flammable, corrosive, n.o.s.	100 m (300 ft)	0.5 km (0.3 mi)	2.5 km (1.6 mi)	500 m (1500 ft)	2.9 km (1.8 mi)	9.2 km (5.7 mi)
3305	**119**	Compressed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)						

3305	**119**	Compressed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)	30 m	(100 ft)	0.2 km	(0.2 mi)	1.0 km	(0.7 mi)	400 m	(1250 ft)	2.3 km	(1.4 mi)	5.1 km	(3.2 mi)
3305	**119**	Compressed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.5 km	(0.3 mi)	300 m	(1000 ft)	1.6 km	(1.0 mi)	3.2 km	(2.0 mi)
3305	**119**	Compressed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone D)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	150 m	(500 ft)	0.8 km	(0.5 mi)	2.0 km	(1.3 mi)
3305	**119**	Compressed gas, toxic, flammable, corrosive, n.o.s.												
3305	**119**	Compressed gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)	100 m	(300 ft)	0.5 km	(0.3 mi)	2.5 km	(1.6 mi)	500 m	(1500 ft)	2.9 km	(1.8 mi)	9.2 km	(5.7 mi)
3305	**119**	Compressed gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)	30 m	(100 ft)	0.2 km	(0.2 mi)	1.0 km	(0.7 mi)	400 m	(1250 ft)	2.3 km	(1.4 mi)	5.1 km	(3.2 mi)
3305	**119**	Compressed gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.5 km	(0.3 mi)	300 m	(1000 ft)	1.6 km	(1.0 mi)	3.2 km	(2.0 mi)
3305	**119**	Compressed gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone D)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	150 m	(500 ft)	0.8 km	(0.5 mi)	2.0 km	(1.3 mi)
3306	**124**	Compressed gas, poisonous, oxidizing, corrosive, n.o.s.												
3306	**124**	Compressed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone A)	100 m	(300 ft)	0.5 km	(0.3 mi)	2.5 km	(1.6 mi)	500 m	(1500 ft)	2.9 km	(1.8 mi)	9.2 km	(5.7 mi)
3306	**124**	Compressed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone B)	30 m	(100 ft)	0.2 km	(0.2 mi)	1.0 km	(0.7 mi)	400 m	(1250 ft)	2.3 km	(1.4 mi)	5.1 km	(3.2 mi)

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
3306	124	Compressed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone C)	30 m (100 ft)	0.1 km (0.1 mi)	0.5 km (0.3 mi)	300 m (1000 ft)	1.6 km (1.0 mi)	3.2 km (2.0 mi)
3306	124	Compressed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone D)	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	150 m (500 ft)	0.8 km (0.5 mi)	2.0 km (1.3 mi)
3306	124	Compressed gas, toxic, oxidizing, corrosive, n.o.s.						
3306	124	Compressed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone A)	100 m (300 ft)	0.5 km (0.3 mi)	2.5 km (1.6 mi)	500 m (1500 ft)	2.9 km (1.8 mi)	9.2 km (5.7 mi)
3306	124	Compressed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone B)	30 m (100 ft)	0.2 km (0.2 mi)	1.0 km (0.7 mi)	400 m (1250 ft)	2.3 km (1.4 mi)	5.1 km (3.2 mi)
3306	124	Compressed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone C)	30 m (100 ft)	0.1 km (0.1 mi)	0.5 km (0.3 mi)	300 m (1000 ft)	1.6 km (1.0 mi)	3.2 km (2.0 mi)
3306	124	Compressed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone D)	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	150 m (500 ft)	0.8 km (0.5 mi)	2.0 km (1.3 mi)

3307	**124**	Liquefied gas, poisonous, oxidizing, n.o.s.												
3307	**124**	Liquefied gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone A)	100 m	(300 ft)	0.5 km	(0.3 mi)	2.5 km	(1.6 mi)	800 m	(2500 ft)	5.0 km	(3.1 mi)	11.0+ km	(7.0+ mi)
3307	**124**	Liquefied gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone B)	60 m	(200 ft)	0.3 km	(0.2 mi)	1.1 km	(0.7 mi)	400 m	(1250 ft)	2.5 km	(1.5 mi)	6.7 km	(4.2 mi)
3307	**124**	Liquefied gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	150 m	(500 ft)	1.0 km	(0.6 mi)	2.9 km	(1.8 mi)
3307	**124**	Liquefied gas, poisonous, oxidizing, n.o.s. (Inhalation Hazard Zone D)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	150 m	(500 ft)	0.8 km	(0.5 mi)	2.0 km	(1.3 mi)
3307	**124**	Liquefied gas, toxic, oxidizing, n.o.s.												
3307	**124**	Liquefied gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone A)	100 m	(300 ft)	0.5 km	(0.3 mi)	2.5 km	(1.6 mi)	800 m	(2500 ft)	5.0 km	(3.1 mi)	11.0+ km	(7.0+ mi)
3307	**124**	Liquefied gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone B)	60 m	(200 ft)	0.3 km	(0.2 mi)	1.1 km	(0.7 mi)	400 m	(1250 ft)	2.5 km	(1.5 mi)	6.7 km	(4.2 mi)
3307	**124**	Liquefied gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	150 m	(500 ft)	1.0 km	(0.6 mi)	2.9 km	(1.8 mi)
3307	**124**	Liquefied gas, toxic, oxidizing, n.o.s. (Inhalation Hazard Zone D)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	150 m	(500 ft)	0.8 km	(0.5 mi)	2.0 km	(1.3 mi)

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
3308	125	Liquefied gas, poisonous, corrosive, n.o.s.						
3308	125	Liquefied gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone A)	100 m (300 ft)	0.5 km (0.3 mi)	2.5 km (1.6 mi)	500 m (1500 ft)	2.9 km (1.8 mi)	9.2 km (5.7 mi)
3308	125	Liquefied gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone B)	30 m (100 ft)	0.2 km (0.2 mi)	1.0 km (0.7 mi)	400 m (1250 ft)	2.3 km (1.4 mi)	5.1 km (3.2 mi)
3308	125	Liquefied gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone C)	30 m (100 ft)	0.1 km (0.1 mi)	0.5 km (0.3 mi)	300 m (1000 ft)	1.6 km (1.0 mi)	3.2 km (2.0 mi)
3308	125	Liquefied gas, poisonous, corrosive, n.o.s. (Inhalation Hazard Zone D)	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	150 m (500 ft)	0.8 km (0.5 mi)	2.0 km (1.3 mi)
3308	125	Liquefied gas, toxic, corrosive, n.o.s.						
3308	125	Liquefied gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone A)	100 m (300 ft)	0.5 km (0.3 mi)	2.5 km (1.6 mi)	500 m (1500 ft)	2.9 km (1.8 mi)	9.2 km (5.7 mi)
3308	125	Liquefied gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone B)	30 m (100 ft)	0.2 km (0.2 mi)	1.0 km (0.7 mi)	400 m (1250 ft)	2.3 km (1.4 mi)	5.1 km (3.2 mi)

3308	**125**	Liquefied gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.5 km	(0.3 mi)	300 m	(1000 ft)	1.6 km	(1.0 mi)	3.2 km	(2.0 mi)
3308	**125**	Liquefied gas, toxic, corrosive, n.o.s. (Inhalation Hazard Zone D)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	150 m	(500 ft)	0.8 km	(0.5 mi)	2.0 km	(1.3 mi)
3309	**119**	Liquefied gas, poisonous, flammable, corrosive, n.o.s.												
3309	**119**	Liquefied gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)	100 m	(300 ft)	0.5 km	(0.3 mi)	2.5 km	(1.6 mi)	500 m	(1500 ft)	2.9 km	(1.8 mi)	9.2 km	(5.7 mi)
3309	**119**	Liquefied gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)	30 m	(100 ft)	0.2 km	(0.2 mi)	1.0 km	(0.7 mi)	400 m	(1250 ft)	2.3 km	(1.4 mi)	5.1 km	(3.2 mi)
3309	**119**	Liquefied gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.5 km	(0.3 mi)	300 m	(1000 ft)	1.6 km	(1.0 mi)	3.2 km	(2.0 mi)
3309	**119**	Liquefied gas, poisonous, flammable, corrosive, n.o.s. (Inhalation Hazard Zone D)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	150 m	(500 ft)	0.8 km	(0.5 mi)	2.0 km	(1.3 mi)
3309	**119**	Liquefied gas, toxic, flammable, corrosive, n.o.s.												
3309	**119**	Liquefied gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)	100 m	(300 ft)	0.5 km	(0.3 mi)	2.5 km	(1.6 mi)	500 m	(1500 ft)	2.9 km	(1.8 mi)	9.2 km	(5.7 mi)
3309	**119**	Liquefied gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)	30 m	(100 ft)	0.2 km	(0.2 mi)	1.0 km	(0.7 mi)	400 m	(1250 ft)	2.3 km	(1.4 mi)	5.1 km	(3.2 mi)
3309	**119**	Liquefied gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.5 km	(0.3 mi)	300 m	(1000 ft)	1.6 km	(1.0 mi)	3.2 km	(2.0 mi)

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
3309	**119**	Liquefied gas, toxic, flammable, corrosive, n.o.s. (Inhalation Hazard Zone D)	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	150 m (500 ft)	0.8 km (0.5 mi)	2.0 km (1.3 mi)
3310	**124**	Liquefied gas, poisonous, oxidizing, corrosive, n.o.s.						
3310	**124**	Liquefied gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone A)	100 m (300 ft)	0.5 km (0.3 mi)	2.5 km (1.6 mi)	500 m (1500 ft)	2.9 km (1.8 mi)	9.2 km (5.7 mi)
3310	**124**	Liquefied gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone B)	30 m (100 ft)	0.2 km (0.2 mi)	1.0 km (0.7 mi)	400 m (1250 ft)	2.3 km (1.4 mi)	5.1 km (3.2 mi)
3310	**124**	Liquefied gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone C)	30 m (100 ft)	0.1 km (0.1 mi)	0.5 km (0.3 mi)	300 m (1000 ft)	1.6 km (1.0 mi)	3.2 km (2.0 mi)
3310	**124**	Liquefied gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone D)	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	150 m (500 ft)	0.8 km (0.5 mi)	2.0 km (1.3 mi)
3310	**124**	Liquefied gas, toxic, oxidizing, corrosive, n.o.s.						
3310	**124**	Liquefied gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone A)	100 m (300 ft)	0.5 km (0.3 mi)	2.5 km (1.6 mi)	500 m (1500 ft)	2.9 km (1.8 mi)	9.2 km (5.7 mi)

3310	**124**	Liquefied gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone B)	30 m	(100 ft)	0.2 km	(0.2 mi)	1.0 km	(0.7 mi)	400 m	(1250 ft)	2.3 km	(1.4 mi)	5.1 km	(3.2 mi)
3310	**124**	Liquefied gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.5 km	(0.3 mi)	300 m	(1000 ft)	1.6 km	(1.0 mi)	3.2 km	(2.0 mi)
3310	**124**	Liquefied gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation Hazard Zone D)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	150 m	(500 ft)	0.8 km	(0.5 mi)	2.0 km	(1.3 mi)
3318	**125**	Ammonia solution, with more than 50% Ammonia	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	150 m	(500 ft)	0.8 km	(0.5 mi)	2.1 km	(1.3 mi)
3355	**119**	Insecticide gas, poisonous, flammable, n.o.s.	150 m	(500 ft)	1.0 km	(0.6 mi)	3.8 km	(2.4 mi)	1000 m	(3000 ft)	5.7 km	(3.6 mi)	10.1 km	(6.3 mi)
3355	**119**	Insecticide gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone A)												
3355	**119**	Insecticide gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone B)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.4 km	(0.2 mi)	300 m	(1000 ft)	1.3 km	(0.8 mi)	3.4 km	(2.1 mi)
3355	**119**	Insecticide gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	150 m	(500 ft)	1.0 km	(0.6 mi)	2.9 km	(1.8 mi)
3355	**119**	Insecticide gas, poisonous, flammable, n.o.s. (Inhalation Hazard Zone D)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	150 m	(500 ft)	0.8 km	(0.5 mi)	2.0 km	(1.3 mi)
3355	**119**	Insecticide gas, toxic, flammable, n.o.s.	150 m	(500 ft)	1.0 km	(0.6 mi)	3.8 km	(2.4 mi)	1000 m	(3000 ft)	5.7 km	(3.6 mi)	10.1 km	(6.3 mi)
3355	**119**	Insecticide gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone A)												

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
3355	**119**	Insecticide gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone B)	30 m (100 ft)	0.1 km (0.1 mi)	0.4 km (0.2 mi)	300 m (1000 ft)	1.3 km (0.8 mi)	3.4 km (2.1 mi)
3355	**119**	Insecticide gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone C)	30 m (100 ft)	0.1 km (0.1 mi)	0.3 km (0.2 mi)	150 m (500 ft)	1.0 km (0.6 mi)	2.9 km (1.8 mi)
3355	**119**	Insecticide gas, toxic, flammable, n.o.s. (Inhalation Hazard Zone D)	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	150 m (500 ft)	0.8 km (0.5 mi)	2.0 km (1.3 mi)
3361	**156**	Chlorosilanes, poisonous, corrosive, n.o.s. **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	60 m (200 ft)	0.5 km (0.3 mi)	1.6 km (1.0 mi)
3361	**156**	Chlorosilanes, toxic, corrosive, n.o.s. **(when spilled in water)**						
3362	**155**	Chlorosilanes, poisonous, corrosive, flammable, n.o.s. **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.1 mi)	60 m (200 ft)	0.5 km (0.3 mi)	1.6 km (1.0 mi)
3362	**155**	Chlorosilanes, toxic, corrosive, flammable, n.o.s. **(when spilled in water)**						
3381	**151**	Poisonous by inhalation liquid, n.o.s. (Inhalation Hazard Zone A)	60 m (200 ft)	0.6 km (0.4 mi)	1.2 km (0.8 mi)	200 m (600 ft)	2.2 km (1.4 mi)	4.2 km (2.6 mi)
3381	**151**	Toxic by inhalation liquid, n.o.s. (Inhalation Hazard Zone A)						

3382	**151**	Poisonous by inhalation liquid, n.o.s. (Inhalation Hazard Zone B)	30 m	(100 ft)	0.2 km	(0.1 mi)	0.2 km	(0.2 mi)	60 m	(200 ft)	0.5 km	(0.3 mi)	0.7 km	(0.5 mi)
3382	**151**	Toxic by inhalation liquid, n.o.s. (Inhalation Hazard Zone B)												
3383	**131**	Poisonous by inhalation liquid, flammable, n.o.s. (Inhalation Hazard Zone A)	60 m	(200 ft)	0.5 km	(0.3 mi)	1.5 km	(0.9 mi)	300 m	(1000 ft)	3.1 km	(2.0 mi)	5.8 km	(3.6 mi)
3383	**131**	Toxic by inhalation liquid, flammable, n.o.s. (Inhalation Hazard Zone A)												
3384	**131**	Poisonous by inhalation liquid, flammable, n.o.s. (Inhalation Hazard Zone B)	30 m	(100 ft)	0.2 km	(0.1 mi)	0.3 km	(0.2 mi)	60 m	(200 ft)	0.6 km	(0.4 mi)	1.0 km	(0.6 mi)
3384	**131**	Toxic by inhalation liquid, flammable, n.o.s. (Inhalation Hazard Zone B)												
3385	**139**	Poisonous by inhalation liquid, water-reactive, n.o.s. (Inhalation Hazard Zone A)	60 m	(200 ft)	0.6 km	(0.4 mi)	1.2 km	(0.8 mi)	200 m	(600 ft)	2.2 km	(1.4 mi)	4.2 km	(2.6 mi)
3385	**139**	Toxic by inhalation liquid, water-reactive, n.o.s. (Inhalation Hazard Zone A)												
3386	**139**	Poisonous by inhalation liquid, water-reactive, n.o.s. (Inhalation Hazard Zone B)	30 m	(100 ft)	0.2 km	(0.1 mi)	0.2 km	(0.2 mi)	60 m	(200 ft)	0.5 km	(0.3 mi)	0.7 km	(0.5 mi)
3386	**139**	Toxic by inhalation liquid, water-reactive, n.o.s. (Inhalation Hazard Zone B)												

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
3387	142	Poisonous by inhalation liquid, oxidizing, n.o.s. (Inhalation Hazard Zone A)	60 m (200 ft)	0.6 km (0.4 mi)	1.2 km (0.8 mi)	200 m (600 ft)	2.2 km (1.4 mi)	4.2 km (2.6 mi)
3387	142	Toxic by inhalation liquid, oxidizing, n.o.s. (Inhalation Hazard Zone A)						
3388	142	Poisonous by inhalation liquid, oxidizing, n.o.s. (Inhalation Hazard Zone B)	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.3 km (0.2 mi)	0.4 km (0.3 mi)
3388	142	Toxic by inhalation liquid, oxidizing, n.o.s. (Inhalation Hazard Zone B)						
3389	154	Poisonous by inhalation liquid, corrosive, n.o.s. (Inhalation Hazard Zone A)	100 m (300 ft)	0.3 km (0.2 mi)	0.8 km (0.5 mi)	400 m (1250 ft)	1.4 km (0.9 mi)	3.3 km (2.1 mi)
3389	154	Toxic by inhalation liquid, corrosive, n.o.s. (Inhalation Hazard Zone A)						
3390	154	Poisonous by inhalation liquid, corrosive, n.o.s. (Inhalation Hazard Zone B)	30 m (100 ft)	0.2 km (0.1 mi)	0.2 km (0.1 mi)	30 m (100 ft)	0.4 km (0.3 mi)	0.6 km (0.4 mi)
3390	154	Toxic by inhalation liquid, corrosive, n.o.s. (Inhalation Hazard Zone B)						

3456	**157**	Nitrosylsulfuric acid, solid **(when spilled in water)**	30 m	(100 ft)	0.1 km	(0.1 mi)	0.3 km	(0.2 mi)	300 m	(1000 ft)	1.0 km	(0.6 mi)	2.9 km	(1.8 mi)
3456	**157**	Nitrosylsulphuric acid, solid **(when spilled in water)**												
3488	**131**	Poisonous by inhalation liquid, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)	100 m	(300 ft)	0.9 km	(0.6 mi)	2.0 km	(1.2 mi)	400 m	(1250 ft)	4.8 km	(3.0 mi)	7.5 km	(4.7 mi)
3488	**131**	Toxic by inhalation liquid, flammable, corrosive, n.o.s. (Inhalation Hazard Zone A)												
3489	**131**	Poisonous by inhalation liquid, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)	30 m	(100 ft)	0.2 km	(0.1 mi)	0.3 km	(0.2 mi)	60 m	(200 ft)	0.6 km	(0.4 mi)	1.0 km	(0.6 mi)
3489	**131**	Toxic by inhalation liquid, flammable, corrosive, n.o.s. (Inhalation Hazard Zone B)												
3490	**155**	Poisonous by inhalation liquid, water-reactive, flammable, n.o.s. (Inhalation Hazard Zone A)	60 m	(200 ft)	0.5 km	(0.3 mi)	1.5 km	(0.9 mi)	300 m	(1000 ft)	3.1 km	(2.0 mi)	5.8 km	(3.6 mi)
3490	**155**	Toxic by inhalation liquid, water-reactive, flammable, n.o.s. (Inhalation Hazard Zone A)												
3491	**155**	Poisonous by inhalation liquid, water-reactive, flammable, n.o.s. (Inhalation Hazard Zone B)	30 m	(100 ft)	0.2 km	(0.1 mi)	0.3 km	(0.2 mi)	60 m	(200 ft)	0.6 km	(0.4 mi)	1.0 km	(0.6 mi)
3491	**155**	Toxic by inhalation liquid, water-reactive, flammable, n.o.s. (Inhalation Hazard Zone B)												

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
3492	**131**	Poisonous by inhalation liquid, corrosive, flammable, n.o.s. (Inhalation Hazard Zone A)	100 m (300 ft)	0.9 km (0.6 mi)	2.0 km (1.2 mi)	400 m (1250 ft)	4.8 km (3.0 mi)	7.5 km (4.7 mi)
3492	**131**	Toxic by inhalation liquid, corrosive, flammable, n.o.s. (Inhalation Hazard Zone A)						
3493	**131**	Poisonous by inhalation liquid, corrosive, flammable, n.o.s. (Inhalation Hazard Zone B)	30 m (100 ft)	0.2 km (0.1 mi)	0.3 km (0.2 mi)	60 m (200 ft)	0.6 km (0.4 mi)	1.0 km (0.6 mi)
3493	**131**	Toxic by inhalation liquid, corrosive, flammable, n.o.s. (Inhalation Hazard Zone B)						
3494	**131**	Petroleum sour crude oil, flammable, poisonous	30 m (100 ft)	0.2 km (0.1 mi)	0.2 km (0.2 mi)	60 m (200 ft)	0.5 km (0.3 mi)	0.7 km (0.5 mi)
3494	**131**	Petroleum sour crude oil, flammable, toxic						
3507	**166**	Uranium hexafluoride, radioactive material, excepted package, less than 0.1 kg per package, non-fissile or fissile-excepted **(when spilled in water)**	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)

3512	**173**	Adsorbed gas, poisonous, n.o.s.	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.2 mi)
3512	**173**	Adsorbed gas, poisonous, n.o.s. (Inhalation hazard zone A)												
3512	**173**	Adsorbed gas, poisonous, n.o.s. (Inhalation hazard zone B)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)
3512	**173**	Adsorbed gas, poisonous, n.o.s. (Inhalation hazard zone C)												
3512	**173**	Adsorbed gas, poisonous, n.o.s. (Inhalation hazard zone D)												
3512	**173**	Adsorbed gas, toxic, n.o.s.	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.2 mi)
3512	**173**	Adsorbed gas, toxic, n.o.s. (Inhalation hazard zone A)												
3512	**173**	Adsorbed gas, toxic, n.o.s. (Inhalation hazard zone B)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)
3512	**173**	Adsorbed gas, toxic, n.o.s. (Inhalation hazard zone C)												
3512	**173**	Adsorbed gas, toxic, n.o.s. (Inhalation hazard zone D)												
3514	**173**	Adsorbed gas, poisonous, flammable, n.o.s.	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.2 mi)
3514	**173**	Adsorbed gas, poisonous, flammable, n.o.s. (Inhalation hazard zone A)												

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
3514	173	Adsorbed gas, poisonous, flammable, n.o.s. (Inhalation hazard zone B)	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)
3514	173	Adsorbed gas, poisonous, flammable, n.o.s. (Inhalation hazard zone C)						
3514	173	Adsorbed gas, poisonous, flammable, n.o.s. (Inhalation hazard zone D)						
3514	173	Adsorbed gas, toxic, flammable, n.o.s.	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.2 mi)
3514	173	Adsorbed gas, toxic, flammable, n.o.s. (Inhalation hazard zone A)						
3514	173	Adsorbed gas, toxic, flammable, n.o.s. (Inhalation hazard zone B)	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)
3514	173	Adsorbed gas, toxic, flammable, n.o.s. (Inhalation hazard zone C)						
3514	173	Adsorbed gas, toxic, flammable, n.o.s. (Inhalation hazard zone D)						

3515	**173**	Adsorbed gas, poisonous, oxidizing, n.o.s.										
3515	**173**	Adsorbed gas, poisonous, oxidizing, n.o.s. (Inhalation hazard zone A)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.2 mi)
3515	**173**	Adsorbed gas, poisonous, oxidizing, n.o.s. (Inhalation hazard zone B)										
3515	**173**	Adsorbed gas, poisonous, oxidizing, n.o.s. (Inhalation hazard zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)
3515	**173**	Adsorbed gas, poisonous, oxidizing, n.o.s. (Inhalation hazard zone D)										
3515	**173**	Adsorbed gas, toxic, oxidizing, n.o.s.										
3515	**173**	Adsorbed gas, toxic, oxidizing, n.o.s. (Inhalation hazard zone A)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.2 mi)
3515	**173**	Adsorbed gas, toxic, oxidizing, n.o.s. (Inhalation hazard zone B)										
3515	**173**	Adsorbed gas, toxic, oxidizing, n.o.s. (Inhalation hazard zone C)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)
3515	**173**	Adsorbed gas, toxic, oxidizing, n.o.s. (Inhalation hazard zone D)										
3516	**173**	Adsorbed gas, poisonous, corrosive, n.o.s.										
3516	**173**	Adsorbed gas, poisonous, corrosive, n.o.s. (Inhalation hazard zone A)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.2 mi)

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
3516	173	Adsorbed gas, poisonous, corrosive, n.o.s. (Inhalation hazard zone B)	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)
3516	173	Adsorbed gas, poisonous, corrosive, n.o.s. (Inhalation hazard zone C)						
3516	173	Adsorbed gas, poisonous, corrosive, n.o.s. (Inhalation hazard zone D)						
3516	173	Adsorbed gas, toxic, corrosive, n.o.s.	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.2 mi)
3516	173	Adsorbed gas, toxic, corrosive, n.o.s. (Inhalation hazard zone A)						
3516	173	Adsorbed gas, toxic, corrosive, n.o.s. (Inhalation hazard zone B)	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)
3516	173	Adsorbed gas, toxic, corrosive, n.o.s. (Inhalation hazard zone C)						
3516	173	Adsorbed gas, toxic, corrosive, n.o.s. (Inhalation hazard zone D)						
3517	173	Adsorbed gas, poisonous, flammable, corrosive, n.o.s.	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.2 mi)
3517	173	Adsorbed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation hazard zone A)						

3517	**173**	Adsorbed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation hazard zone B)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)
3517	**173**	Adsorbed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation hazard zone C)												
3517	**173**	Adsorbed gas, poisonous, flammable, corrosive, n.o.s. (Inhalation hazard zone D)												
3517	**173**	Adsorbed gas, toxic, flammable, corrosive, n.o.s	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.2 mi)
3517	**173**	Adsorbed gas, toxic, flammable, corrosive, n.o.s. (Inhalation hazard zone A)												
3517	**173**	Adsorbed gas, toxic, flammable, corrosive, n.o.s. (Inhalation hazard zone B)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)
3517	**173**	Adsorbed gas, toxic, flammable, corrosive, n.o.s. (Inhalation hazard zone C)												
3517	**173**	Adsorbed gas, toxic, flammable, corrosive, n.o.s. (Inhalation hazard zone D)												
3518	**173**	Adsorbed gas, poisonous, oxidizing, corrosive, n.o.s	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.2 mi)
3518	**173**	Adsorbed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation hazard zone A)												

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

TABLE 1 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES

ID No.	Guide	NAME OF MATERIAL	SMALL SPILLS (From a small package or small leak from a large package) First ISOLATE in all Directions Meters (Feet)	SMALL SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	SMALL SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)	LARGE SPILLS (From a large package or from many small packages) First ISOLATE in all Directions Meters (Feet)	LARGE SPILLS Then PROTECT persons Downwind during DAY Kilometers (Miles)	LARGE SPILLS Then PROTECT persons Downwind during NIGHT Kilometers (Miles)
3518	173	Adsorbed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation hazard zone B)	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)
3518	173	Adsorbed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation hazard zone C)						
3518	173	Adsorbed gas, poisonous, oxidizing, corrosive, n.o.s. (Inhalation hazard zone D)						
3518	173	Adsorbed gas, toxic, oxidizing, corrosive, n.o.s.	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.1 km (0.1 mi)	0.2 km (0.2 mi)
3518	173	Adsorbed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation hazard zone A)						
3518	173	Adsorbed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation hazard zone B)	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)
3518	173	Adsorbed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation hazard zone C)						
3518	173	Adsorbed gas, toxic, oxidizing, corrosive, n.o.s. (Inhalation hazard zone D)						
3519	173	Boron trifluoride, adsorbed	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)
3520	173	Chlorine, adsorbed	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)	30 m (100 ft)	0.1 km (0.1 mi)	0.1 km (0.1 mi)

3521	**173**	Silicon tetrafluoride, adsorbed	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)
3522	**173**	Arsine, adsorbed	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.2 mi)
3523	**173**	Germane, adsorbed	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.2 mi)
3524	**173**	Phosphorus pentafluoride, adsorbed	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)
3525	**173**	Phosphine, adsorbed	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)
3526	**173**	Hydrogen selenide, adsorbed	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.4 km	(0.3 mi)
3539	**123**	Articles containing toxic gas, n.o.s.	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.4 km	(0.3 mi)
9191	**143**	Chlorine dioxide, hydrate, frozen (**when spilled in water**)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.2 km	(0.1 mi)	0.5 km	(0.3 mi)
9202	**168**	Carbon monoxide, refrigerated liquid (cryogenic liquid)	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	200 m	(600 ft)	1.2 km	(0.7 mi)	4.3 km	(2.7 mi)
9206	**137**	Methyl phosphonic dichloride	30 m	(100 ft)	0.1 km	(0.1 mi)	0.2 km	(0.1 mi)	30 m	(100 ft)	0.4 km	(0.3 mi)	0.6 km	(0.4 mi)
9263	**156**	Chloropivaloyl chloride	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.2 km	(0.2 mi)	0.3 km	(0.2 mi)
9264	**151**	3,5-Dichloro-2,4,6-trifluoropyridine	30 m	(100 ft)	0.1 km	(0.1 mi)	0.1 km	(0.1 mi)	30 m	(100 ft)	0.2 km	(0.2 mi)	0.3 km	(0.2 mi)
9269	**132**	Trimethoxysilane	30 m	(100 ft)	0.2 km	(0.2 mi)	0.6 km	(0.4 mi)	100 m	(300 ft)	1.3 km	(0.8 mi)	2.3 km	(1.5 mi)

See Next Page for Table of Water-Reactive Materials Which Produce Toxic Gases

"+" means distance can be larger in certain atmospheric conditions

TABLE 1

HOW TO USE TABLE 2 – WATER-REACTIVE MATERIALS THAT PRODUCE TOXIC GASES

Table 2 lists materials that produce large amounts of Toxic Inhalation Hazard (TIH) (PIH in the US) gases when spilled in water, and identifies the TIH gases produced.

The materials are listed by order of ID number.

These Water-Reactive materials are easily identified in Table 1 as their name is immediately followed by **(when spilled in water)**.

Note 1: The TIH gases indicated in Table 2 are for information purposes only. In Table 1, the initial isolation and protective action distances have already taken into consideration the TIH gases produced.

For example: Table 2 indicates that UN1689 sodium cyanide, when spilled in water, will generate hydrogen cyanide gas (HCN). In Table 1, you must refer to the distances for sodium cyanide and not the distances for hydrogen cyanide gas.

Note 2: Some Water-Reactive materials are also TIH materials themselves (e.g., UN1746 (Bromine trifluoride), UN1836 (Thionyl chloride)). In these instances, two entries are provided in Table 1 for land-based and water-based spills. If a water-reactive material only has one entry in Table 1 for **(when spilled in water)**, and the product is **NOT** spilled in water, Tables 1 and 2 do **NOT** apply. Refer only to the appropriate orange-bordered guide.

Note 3: Materials classified as a Division 4.3 are substances that, on contact with water, are liable to become spontaneously **FLAMMABLE** or give off **FLAMMABLE** or sometimes **TOXIC** gases in dangerous quantities. For the purpose of this table, water-reactive materials are materials that generate substantial quantities of **TOXIC** gases rapidly after a spill into water; therefore, a material classified as a Division 4.3 will not always be included in Table 2.

Materials Which Produce Large Amounts of Toxic-by-Inhalation (TIH) (PIH in the US) Gas(es) When Spilled in Water

ID No.	Guide No.	Name of Material	TIH Gas(es) Produced
1162	**155**	Dimethyldichlorosilane	HCl
1183	**139**	Ethyldichlorosilane	HCl
1196	**155**	Ethyltrichlorosilane	HCl
1242	**139**	Methyldichlorosilane	HCl
1250	**155**	Methyltrichlorosilane	HCl
1295	**139**	Trichlorosilane	HCl
1298	**155**	Trimethylchlorosilane	HCl
1305	**155P**	Vinyltrichlorosilane	HCl
1305	**155P**	Vinyltrichlorosilane, stabilized	HCl
1340	**139**	Phosphorus pentasulfide, free from yellow and white Phosphorus	H_2S
1340	**139**	Phosphorus pentasulphide, free from yellow and white Phosphorus	H_2S
1360	**139**	Calcium phosphide	PH_3
1384	**135**	Sodium dithionite	H_2S SO_2
1384	**135**	Sodium hydrosulfite	H_2S SO_2
1384	**135**	Sodium hydrosulphite	H_2S SO_2
1390	**139**	Alkali metal amides	NH_3
1397	**139**	Aluminum phosphide	PH_3
1419	**139**	Magnesium aluminum phosphide	PH_3
1432	**139**	Sodium phosphide	PH_3
1541	**155**	Acetone cyanohydrin, stabilized	HCN
1680	**157**	Potassium cyanide, solid	HCN
1689	**157**	Sodium cyanide, solid	HCN

Chemical Symbols for TIH (PIH in the US) Gases:

Br_2	Bromine	HF	Hydrogen fluoride	NO_2	Nitrogen dioxide
Cl_2	Chlorine	HI	Hydrogen iodide	PH_3	Phosphine
HBr	Hydrogen bromide	H_2S	Hydrogen sulfide	SO_2	Sulfur dioxide
HCl	Hydrogen chloride	H_2S	Hydrogen sulphide	SO_2	Sulphur dioxide
HCN	Hydrogen cyanide	NH_3	Ammonia		

TABLE 2 - WATER-REACTIVE MATERIALS WHICH PRODUCE TOXIC GASES

Materials Which Produce Large Amounts of Toxic-by-Inhalation (TIH) (PIH in the US) Gas(es) When Spilled in Water

ID No.	Guide No.	Name of Material	TIH Gas(es) Produced
1716	**156**	Acetyl bromide	HBr
1717	**155**	Acetyl chloride	HCl
1724	**155**	Allyltrichlorosilane, stabilized	HCl
1725	**137**	Aluminum bromide, anhydrous	HBr
1726	**137**	Aluminum chloride, anhydrous	HCl
1728	**155**	Amyltrichlorosilane	HCl
1732	**157**	Antimony pentafluoride	HF
1741	**125**	Boron trichloride	HCl
1745	**144**	Bromine pentafluoride	HF Br_2
1746	**144**	Bromine trifluoride	HF Br_2
1747	**155**	Butyltrichlorosilane	HCl
1752	**156**	Chloroacetyl chloride	HCl
1753	**156**	Chlorophenyltrichlorosilane	HCl
1754	**137**	Chlorosulfonic acid (with or without sulfur trioxide)	HCl
1754	**137**	Chlorosulphonic acid (with or without sulphur trioxide)	HCl
1758	**137**	Chromium oxychloride	HCl
1762	**156**	Cyclohexenyltrichlorosilane	HCl
1763	**156**	Cyclohexyltrichlorosilane	HCl
1765	**156**	Dichloroacetyl chloride	HCl
1766	**156**	Dichlorophenyltrichlorosilane	HCl
1767	**155**	Diethyldichlorosilane	HCl
1769	**156**	Diphenyldichlorosilane	HCl
1771	**156**	Dodecyltrichlorosilane	HCl

Chemical Symbols for TIH (PIH in the US) Gases:

Br_2	Bromine	HF	Hydrogen fluoride	NO_2	Nitrogen dioxide
Cl_2	Chlorine	HI	Hydrogen iodide	PH_3	Phosphine
HBr	Hydrogen bromide	H_2S	Hydrogen sulfide	SO_2	Sulfur dioxide
HCl	Hydrogen chloride	H_2S	Hydrogen sulphide	SO_2	Sulphur dioxide
HCN	Hydrogen cyanide	NH_3	Ammonia		

Use this list only when material is spilled in water.

Materials Which Produce Large Amounts of Toxic-by-Inhalation (TIH) (PIH in the US) Gas(es) When Spilled in Water

ID No.	Guide No.	Name of Material	TIH Gas(es) Produced
1777	**137**	Fluorosulfonic acid	HF
1777	**137**	Fluorosulphonic acid	HF
1781	**156**	Hexadecyltrichlorosilane	HCl
1784	**156**	Hexyltrichlorosilane	HCl
1799	**156**	Nonyltrichlorosilane	HCl
1800	**156**	Octadecyltrichlorosilane	HCl
1801	**156**	Octyltrichlorosilane	HCl
1804	**156**	Phenyltrichlorosilane	HCl
1806	**137**	Phosphorus pentachloride	HCl
1808	**137**	Phosphorus tribromide	HBr
1809	**137**	Phosphorus trichloride	HCl
1810	**137**	Phosphorus oxychloride	HCl
1815	**132**	Propionyl chloride	HCl
1816	**155**	Propyltrichlorosilane	HCl
1818	**157**	Silicon tetrachloride	HCl
1828	**137**	Sulfur chlorides	HCl SO_2 H_2S
1828	**137**	Sulphur chlorides	HCl SO_2 H_2S
1834	**137**	Sulfuryl chloride	HCl
1834	**137**	Sulphuryl chloride	HCl
1836	**137**	Thionyl chloride	HCl SO_2
1838	**137**	Titanium tetrachloride	HCl
1898	**156**	Acetyl iodide	HI
1923	**135**	Calcium dithionite	H_2S SO_2

Chemical Symbols for TIH (PIH in the US) Gases:

Br_2	Bromine	HF	Hydrogen fluoride	NO_2	Nitrogen dioxide
Cl_2	Chlorine	HI	Hydrogen iodide	PH_3	Phosphine
HBr	Hydrogen bromide	H_2S	Hydrogen sulfide	SO_2	Sulfur dioxide
HCl	Hydrogen chloride	H_2S	Hydrogen sulphide	SO_2	Sulphur dioxide
HCN	Hydrogen cyanide	NH_3	Ammonia		

Materials Which Produce Large Amounts of Toxic-by-Inhalation (TIH) (PIH in the US) Gas(es) When Spilled in Water

ID No.	Guide No.	Name of Material	TIH Gas(es) Produced
1923	**135**	Calcium hydrosulfite	H_2S SO_2
1923	**135**	Calcium hydrosulphite	H_2S SO_2
1929	**135**	Potassium dithionite	H_2S SO_2
1929	**135**	Potassium hydrosulfite	H_2S SO_2
1929	**135**	Potassium hydrosulphite	H_2S SO_2
1931	**171**	Zinc dithionite	H_2S SO_2
1931	**171**	Zinc hydrosulfite	H_2S SO_2
1931	**171**	Zinc hydrosulphite	H_2S SO_2
2004	**135**	Magnesium diamide	NH_3
2011	**139**	Magnesium phosphide	PH_3
2012	**139**	Potassium phosphide	PH_3
2013	**139**	Strontium phosphide	PH_3
2308	**157**	Nitrosylsulfuric acid, liquid	NO_2
2308	**157**	Nitrosylsulphuric acid, liquid	NO_2
2353	**132**	Butyryl chloride	HCl
2395	**132**	Isobutyryl chloride	HCl
2434	**156**	Dibenzyldichlorosilane	HCl
2435	**156**	Ethylphenyldichlorosilane	HCl
2437	**156**	Methylphenyldichlorosilane	HCl
2495	**144**	Iodine pentafluoride	HF
2691	**137**	Phosphorus pentabromide	HBr
2692	**157**	Boron tribromide	HBr
2806	**139**	Lithium nitride	NH_3

Chemical Symbols for TIH (PIH in the US) Gases:

Br_2	Bromine	HF	Hydrogen fluoride	NO_2	Nitrogen dioxide
Cl_2	Chlorine	HI	Hydrogen iodide	PH_3	Phosphine
HBr	Hydrogen bromide	H_2S	Hydrogen sulfide	SO_2	Sulfur dioxide
HCl	Hydrogen chloride	H_2S	Hydrogen sulphide	SO_2	Sulphur dioxide
HCN	Hydrogen cyanide	NH_3	Ammonia		

Use this list only when material is spilled in water.

Materials Which Produce Large Amounts of Toxic-by-Inhalation (TIH) (PIH in the US) Gas(es) When Spilled in Water

ID No.	Guide No.	Name of Material	TIH Gas(es) Produced
2965	**139**	Boron trifluoride dimethyl etherate	HF
2977	**166**	Radioactive material, Uranium hexafluoride, fissile	HF
2977	**166**	Uranium hexafluoride, radioactive material, fissile	HF
2978	**166**	Radioactive material, Uranium hexafluoride, non fissile or fissile-excepted	HF
2978	**166**	Uranium hexafluoride, radioactive material, non fissile or fissile-excepted	HF
2985	**155**	Chlorosilanes, flammable, corrosive, n.o.s	HCl
2986	**155**	Chlorosilanes, corrosive, flammable, n.o.s	HCl
2987	**156**	Chlorosilanes, corrosive, n.o.s	HCl
2988	**139**	Chlorosilanes, water-reactive, flammable, corrosive, n.o.s.	HCl
3048	**157**	Aluminum phosphide pesticide	PH_3
3361	**156**	Chlorosilanes, poisonous, corrosive, n.o.s.	HCl
3361	**156**	Chlorosilanes, toxic, corrosive, n.o.s.	HCl
3362	**155**	Chlorosilanes, poisonous, corrosive, flammable, n.o.s.	HCl
3362	**155**	Chlorosilanes, toxic, corrosive, flammable, n.o.s.	HCl
3456	**157**	Nitrosylsulfuric acid, solid	NO_2
3456	**157**	Nitrosylsulphuric acid, solid	NO_2
3507	**166**	Uranium hexafluoride, radioactive material, excepted package, less than 0.1 kg per package, non-fissile or fissile-excepted	HF
9191	**143**	Chlorine dioxide, hydrate, frozen	Cl_2

Chemical Symbols for TIH (PIH in the US) Gases:

Br_2	Bromine	HF	Hydrogen fluoride	NO_2	Nitrogen dioxide
Cl_2	Chlorine	HI	Hydrogen iodide	PH_3	Phosphine
HBr	Hydrogen bromide	H_2S	Hydrogen sulfide	SO_2	Sulfur dioxide
HCl	Hydrogen chloride	H_2S	Hydrogen sulphide	SO_2	Sulphur dioxide
HCN	Hydrogen cyanide	NH_3	Ammonia		

HOW TO USE TABLE 3 – INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES FOR LARGE SPILLS FOR DIFFERENT QUANTITIES OF SIX COMMON TIH (PIH in the US) GASES

Table 3 lists Toxic Inhalation Hazard (TIH) materials that may be more commonly encountered.

The selected materials are:

- UN1005 - Ammonia, anhydrous
- UN1017 - Chlorine
- UN1040 - Ethylene oxide and UN1040 – Ethylene oxide with nitrogen
- UN1050 - Hydrogen chloride, anhydrous and UN2186 - and Hydrogen chloride, refrigerated liquid
- UN1052 - Hydrogen fluoride, anhydrous
- UN1079 - Sulfur dioxide/Sulphur dioxide

The materials are presented in numerical order of ID number and provide Initial Isolation and Protective Action Distances **FOR LARGE SPILLS** (more than 208 liters or 55 US gallons) involving different container types (therefore different volume capacities, see below) for day time and night time situations and different wind speeds.

- Rail tank car: 80 000 kg (176 368 lbs.)
- Highway tank truck or trailer: 20 000 – 25 000 kg (44 092 – 55 115 lbs.)
- Agricultural nurse tank: 3785 L (1000 gallons)
- Small cylinder: 72 L (19 gallons)
- Ton cylinder: 757 - 1135 L (200 - 300 gallons)

Estimating Wind Speed from Environmental Clues

mph	km/h	Wind Description	Specifications
< 6	< 10	Low wind	Wind felt on face; leaves rustle; ordinary vane moved by wind
6 - 12	10 - 20	Moderate wind	Raises dust, loose paper; small branches are moved
> 12	> 20	High wind	Large branches in motion; whistling heard in telephone wires; umbrellas used with difficulty

(Data taken from the Beaufort Wind Scale has been reworked in order to create 3 categories of wind speed: Low, Moderate and High)

TABLE 3 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES FOR LARGE SPILLS FOR DIFFERENT QUANTITIES OF SIX COMMON TIH (PIH in the US) GASES

	First **ISOLATE** in all Directions		Then **PROTECT** persons Downwind during											
			DAY						**NIGHT**					
			Low wind (< 6 mph = < 10 km/h)		Moderate wind (6-12 mph = 10 - 20 km/h)		High wind (> 12 mph = > 20 km/h)		Low wind (< 6 mph = < 10 km/h)		Moderate wind (6-12 mph = 10 - 20 km/h)		High wind (> 12 mph = > 20 km/h)	
	Meters	(Feet)	km	(Miles)	km	(Miles)	km	(Miles)	km	(Miles)	km	(Miles)	km	(Miles)
TRANSPORT CONTAINER	**UN1005 Ammonia, anhydrous: Large Spills**													
Rail tank car	300	(1000)	1.9	(1.2)	1.5	(0.9)	1.1	(0.6)	4.5	(2.8)	2.5	(1.5)	1.4	(0.9)
Highway tank truck or trailer	150	(500)	0.9	(0.6)	0.5	(0.3)	0.4	(0.3)	2.0	(1.3)	0.8	(0.5)	0.6	(0.4)
Agricultural nurse tank	60	(200)	0.5	(0.3)	0.3	(0.2)	0.3	(0.2)	1.4	(0.9)	0.3	(0.2)	0.3	(0.2)
Multiple small cylinders	30	(100)	0.3	(0.2)	0.2	(0.1)	0.1	(0.1)	0.7	(0.5)	0.3	(0.2)	0.2	(0.1)
TRANSPORT CONTAINER	**UN1017 Chlorine: Large Spills**													
Rail tank car	1000	(3000)	10.1	(6.3)	6.8	(4.2)	5.3	(3.3)	11+	(7+)	9.2	(5.7)	6.9	(4.3)
Highway tank truck or trailer	600	(2000)	5.8	(3.6)	3.4	(2.1)	2.9	(1.8)	6.7	(4.3)	5.0	(3.1)	4.1	(2.5)
Multiple ton cylinders	300	(1000)	2.1	(1.3)	1.3	(0.8)	1.0	(0.6)	4.0	(2.5)	2.4	(1.5)	1.3	(0.8)
Multiple small cylinders or single ton cylinder	150	(500)	1.5	(0.9)	0.8	(0.5)	0.5	(0.3)	2.9	(1.8)	1.3	(0.8)	0.6	(0.4)

TABLE 3

"+" means distance can be larger in certain atmospheric conditions

TABLE 3 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES FOR LARGE SPILLS FOR DIFFERENT QUANTITIES OF SIX COMMON TIH (PIH in the US) GASES

	First **ISOLATE** in all Directions		Then **PROTECT** persons Downwind during											
			DAY						**NIGHT**					
			Low wind (< 6 mph = < 10 km/h)		Moderate wind (6-12 mph = 10 - 20 km/h)		High wind (> 12 mph = > 20 km/h)		Low wind (< 6 mph = < 10 km/h)		Moderate wind (6-12 mph = 10 - 20 km/h)		High wind (> 12 mph = > 20 km/h)	
	Meters	(Feet)	km	(Miles)	km	(Miles)	km	(Miles)	km	(Miles)	km	(Miles)	km	(Miles)
TRANSPORT CONTAINER	**UN1040 Ethylene oxide: Large Spills UN1040 Ethylene oxide with Nitrogen: Large Spills**													
Rail tank car	200	(600)	1.6	(1.0)	0.8	(0.5)	0.7	(0.5)	3.3	(2.1)	1.4	(0.9)	0.8	(0.5)
Highway tank truck or trailer	100	(300)	0.9	(0.6)	0.5	(0.3)	0.4	(0.3)	2.0	(1.3)	0.7	(0.4)	0.4	(0.3)
Multiple small cylinders or single ton cylinder	30	(100)	0.4	(0.3)	0.2	(0.1)	0.1	(0.1)	0.9	(0.6)	0.3	(0.2)	0.2	(0.1)
TRANSPORT CONTAINER	**UN1050 Hydrogen chloride, anhydrous: Large Spills UN2186 Hydrogen chloride, refrigerated liquid: Large Spills**													
Rail tank car	500	(1500)	3.9	(2.5)	2.1	(1.2)	1.8	(1.2)	10.1	(6.3)	3.5	(2.2)	2.3	(1.5)
Highway tank truck or trailer	200	(600)	1.5	(0.9)	0.8	(0.5)	0.6	(0.4)	3.9	(2.5)	1.5	(0.9)	0.8	(0.5)
Multiple ton cylinders	30	(100)	0.4	(0.3)	0.2	(0.1)	0.1	(0.1)	1.1	(0.7)	0.3	(0.2)	0.2	(0.1)
Multiple small cylinders or single ton cylinder	30	(100)	0.3	(0.2)	0.2	(0.1)	0.1	(0.1)	0.9	(0.6)	0.3	(0.2)	0.2	(0.1)

TABLE 3 - INITIAL ISOLATION AND PROTECTIVE ACTION DISTANCES FOR LARGE SPILLS FOR DIFFERENT QUANTITIES OF SIX COMMON TIH (PIH in the US) GASES

	First **ISOLATE** in all Directions		Then **PROTECT** persons Downwind during											
			DAY						**NIGHT**					
			Low wind (< 6 mph = < 10 km/h)		Moderate wind (6-12 mph = 10 - 20 km/h)		High wind (> 12 mph = > 20 km/h)		Low wind (< 6 mph = < 10 km/h)		Moderate wind (6-12 mph = 10 - 20 km/h)		High wind (> 12 mph = > 20 km/h)	
	Meters	(Feet)	km	(Miles)	km	(Miles)	km	(Miles)	km	(Miles)	km	(Miles)	km	(Miles)
TRANSPORT CONTAINER	**UN1052 Hydrogen fluoride, anhydrous: Large Spills**													
Rail tank car	500	(1500)	3.5	(2.2)	2.1	(1.3)	1.8	(1.2)	6.6	(4.1)	3.1	(1.9)	2.0	(1.2)
Highway tank truck or trailer	200	(700)	2.0	(1.2)	1.0	(0.7)	0.9	(0.6)	3.7	(2.3)	1.6	(1.0)	0.9	(0.6)
Multiple small cylinders or single ton cylinder	100	(300)	0.8	(0.5)	0.4	(0.2)	0.3	(0.2)	1.7	(1.1)	0.5	(0.3)	0.3	(0.2)
TRANSPORT CONTAINER	**UN1079 Sulfur dioxide/Sulphur dioxide: Large Spills**													
Rail tank car	1000	(3000)	11+	(7+)	11+	(7+)	7.2	(4.5)	11+	(7+)	11+	(7+)	10.1	(6.3)
Highway tank truck or trailer	1000	(3000)	11+	(7+)	6.2	(3.8)	5.3	(3.3)	11+	(7+)	8.2	(5.1)	6.2	(3.9)
Multiple ton cylinders	500	(1500)	5.4	(3.4)	2.4	(1.5)	1.8	(1.1)	7.8	(4.8)	4.2	(2.6)	2.9	(1.8)
Multiple small cylinders or single ton cylinder	200	(600)	3.2	(2.0)	1.5	(0.9)	1.1	(0.7)	5.8	(3.6)	2.5	(1.6)	1.5	(0.9)

TABLE 3

"+" means distance can be larger in certain atmospheric conditions

ERG2020 USER'S GUIDE

For the purposes of this guidebook, the terms hazardous materials/dangerous goods are synonymous.

The 2020 Emergency Response Guidebook (ERG2020) was developed jointly by Transport Canada (TC), the U.S. Department of Transportation (DOT), and the Secretariat of Communications and Transport of Mexico (SCT), with help from CIQUIME (Centro de Información Química para Emergencias) of Argentina.

This guidebook is for firefighters, police and other emergency services personnel who may be first to arrive at the scene of a transportation incident involving dangerous goods.

It is primarily a guide to help first responders to quickly:

- **identify the specific or generic hazards of material(s) involved in a transportation incident**
- **protect themselves and the general public during the initial response phase of the incident**

For the purposes of this guidebook, "initial response phase" is the period after first responders arrive at the scene of an incident. During this phase, responders:

- confirm the presence and/or identification of dangerous goods
- start taking protective action and securing the area
- request the help of qualified personnel

This guide is designed for use at a dangerous goods incident on a highway or railroad. It may have limited value at fixed-facility locations, or onboard aircrafts or vessels.

This guide **does not:**

- provide information on the physical or chemical properties of dangerous goods
- replace emergency response training, knowledge, or sound judgment
- address all possible circumstances that may be associated with a dangerous goods incident

ERG2020 incorporates dangerous goods lists from the most recent United Nations Recommendations, and from other international and national regulations.

Explosives are not listed individually (by either proper shipping name or ID number) but, under the general heading "Explosives", they do appear:

- on the first page of the ID Number index (yellow-bordered pages)
- alphabetically in the Name of Material index (blue-bordered pages)

Chemical warfare agents do not have an assigned ID number because they are not commercially transported. In an emergency situation, the assigned guide (orange-bordered pages) will provide guidance for the initial response.

The letter **(P)** following the guide number in the yellow and blue bordered pages identifies materials that present a polymerization hazard under certain conditions. For example: UN1092 - Acrolein, stabilized GUIDE **131P**.

First responders at the scene of a dangerous goods incident should not solely rely on this guidebook. Always seek specific information about any material in question as soon as possible. To do so:

- Contact the appropriate emergency response agency listed on the inside back cover.
- Call the emergency response telephone number on the shipping paper.
- Consult information on or accompanying the shipping paper.

BEFORE AN EMERGENCY – BECOME FAMILIAR WITH THIS GUIDEBOOK! In the U.S., according to the requirements of the U.S. Department of Labor's Occupational Safety and Health Administration (OSHA, 29 CFR 1910.120) and regulations issued by the U.S. Environmental Protection Agency (EPA, 40 CFR Part 311), first responders must be trained in how to use this guidebook.

GUIDEBOOK CONTENTS

1- Yellow-bordered pages: Index list of dangerous goods in order of ID number. The list displays the 4-digit ID followed by its assigned emergency response guide and material name.

For example:	ID No.	GUIDE No.	Name of Material
	1090	127	Acetone

2- Blue-bordered pages: Index list of dangerous goods in alphabetical order of material name. The list displays the name followed by its assigned emergency response guide and 4-digit ID number.

For example:	Name of Material	GUIDE No.	ID No.
	Sulfuric acid	137	1830

3- Orange-bordered pages: All safety recommendations are provided here. It is made up of 62 individual guides in a 2-page format. Each guide recommends safety and emergency response procedures to protect yourself and the public. The left-hand page gives safety-related information and evacuation distances. The right-hand page gives emergency response guidance for fires, spills or leaks, and first aid. Each guide applies to a group of materials with similar chemical and toxicological characteristics. The guide title identifies the general hazards of the dangerous goods.

For example: GUIDE 124 - **Gases - Toxic and/or Corrosive - Oxidizing**.

Each guide is divided into 3 main sections:

POTENTIAL HAZARDS:

- Displays the hazards in terms of **FIRE OR EXPLOSION** and **HEALTH** effects upon exposure.
- Primary potential hazard is listed first.
- Consult this section first to help you make decisions about how to protect the emergency response team and surrounding population.

PUBLIC SAFETY:

- Provides general information on initial precautionary measures to be taken by those first on scene.
- Provides general guidance on **PROTECTIVE CLOTHING** requirements and respiratory protection.
- Lists suggested **EVACUATION** distances for immediate precautionary measures, spills, and for fires (fragmentation hazard).
- When the material is highlighted in green in the yellow and blue bordered pages, it directs the reader to consult Table 1, which lists Toxic Inhalation Hazard (TIH) (PIH in the U.S.) materials, water-reactive materials and chemical warfare agents (green-bordered pages).

EMERGENCY RESPONSE:

- Outlines special precautions for incidents that involve **FIRE**, **SPILL OR LEAK** or chemical exposure.
- Lists several recommendations under each part to further assist your decision-making process.
- Provides general **FIRST AID** guidance to use before seeking medical care.

4- Green-bordered pages: This section has 3 tables.

Table 1 - Initial Isolation and Protective Action Distances

Lists, by order of ID number:

- TIH (PIH in the U.S.) materials
- water-reactive materials that produce toxic gases upon contact with water
- certain chemical warfare agents

These materials are highlighted in green in the yellow and blue bordered pages so you can easily identify them.

Table 1 provides two types of recommended safety distances: **"initial isolation distances"** and **"protective action distances"** for:

- **small spills**: 208 liters (55 US gallons) or less
- **large spills**: more than 208 liters (55 US gallons)
- Exception: For entries marked **(when used as a weapon)**, volumes vary, but in most cases, small spills include releases up to 2 kg (4.4 lbs.), and large spills include releases up to 25 kg (55 lbs.).

Within the **"initial isolation distance"**, protective clothing and respiratory protection is required. You should consider evacuating all people **in all directions** from the spill or leak source. This distance defines the radius of the "initial isolation zone" surrounding the spill in which people may be exposed to:

- dangerous concentrations upwind of the source
- life-threatening concentrations downwind of the source

The **"protective action distances"** are downwind distances from the spill or leak source, within which responders could carry out protective actions to:

- preserve the health and safety of emergency responders and the public
- evacuate and/or shelter-in-place people in this area (For more information, consult pp. 289 to 291)

The "protective action distance" is divided into **daytime** and **nighttime** incidents because varying atmospheric conditions affect a hazardous area's size. In fact, the quantity or concentration of the material's vapor poses problems, not its mere presence. During the night, the air is generally calmer. This causes the vapor to disperse less and therefore creates a greater toxic zone. In daytime, the atmosphere is more active, so the vapor disperses more. As a result, there is a lower concentration of vapor in the surrounding air and the area that reaches toxic levels is smaller. Daytime is after sunrise and before sunset. Nighttime is between sunset and sunrise.

For example, in the case of a small spill of UN1955 - compressed gas, toxic, n.o.s., the **"initial isolation distance"** is 100 meters (300 feet); therefore its "initial isolation zone" is 200 meters (600 feet) in diameter. Its **"protective action distance"** is 0.5 kilometers (0.3 miles) for daytime and 2.5 kilometers (1.6 miles) for nighttime.

Note 1: Some water-reactive materials have 2 entries in Table 1. They are identified by **(when spilled on land)** since they are TIH products and **(when spilled in water)** because they produce additional toxic gases when spilled in water.

For example: UN1746 - Bromine trifluoride and UN1836 - Thionyl chloride.

Note 2: If a water-reactive material only has one entry in Table 1 for **(when spilled in water)** and the product is NOT spilled in water, Table 1 and Table 2 do not apply. You will find safe distances in the appropriate orange-bordered guide.

For example: UN1183 - Ethyldichlorosilane and UN1898 – Acetyl iodide.

Table 2 - Water-Reactive Materials Which Produce Toxic Gases

Lists:

- by order of ID number, materials that produce large amounts of Toxic Inhalation Hazard (TIH) gases when spilled in water; and
- TIH gases produced by these materials.

You can easily identify water-reactive materials in **Table 1,** as their names are immediately followed by **(when spilled in water).**

NOTE: The TIH gases indicated in Table 2 are for information purposes only. These TIH gases have already been taken into consideration in the distances of Table 1.

For example, Table 2 indicates that UN1689 sodium cyanide, when spilled in water, will generate hydrogen cyanide gas (HCN). In Table 1, you must refer to the distances for sodium cyanide, solid and not the distances for hydrogen cyanide gas.

Table 3 - Initial Isolation and Protective Action Distances for Large Spills for Different Quantities of Six Common TIH Gases

Lists the following 6 most common TIH materials:

- UN1005 - Ammonia, anhydrous
- UN1017 - Chlorine
- UN1040 - Ethylene oxide and UN1040 - Ethylene oxide with nitrogen
- UN1050 - Hydrogen chloride, anhydrous and UN2186 - Hydrogen chloride, refrigerated liquid
- UN1052 - Hydrogen fluoride, anhydrous
- UN1079 - Sulfur dioxide/Sulphur dioxide

Table 3 shows:

- initial isolation and protective action distances for large spills (more than 208 liters or 55 US gallons)
- different container types (therefore different volume capacities) for daytime and nighttime, and for three different wind speeds (low, moderate and high)

HOW TO CHOOSE THE APPROPRIATE ISOLATION AND PROTECTIVE ACTION DISTANCES

ERG2020 lists isolation or evacuation distances in 2 places:

- the individual guides (orange-bordered pages)
- Table 1 – Initial Isolation and Protective Action Distances (green-bordered pages)

If you are dealing with a **non-TIH material** (not highlighted in green in the yellow-bordered or blue-bordered pages),

- Go to the assigned guide for the material (orange-bordered pages).
- Under **EVACUATION**, you will find:
  - initial isolation distance as an immediate precautionary measure
  - specific distances for spill or fire situations (fragmentation hazard)
  - **Please note** that certain guides may also refer to Table 1. This is just a reminder for green highlighted materials only.

If you are dealing with a **TIH, water-reactive** or **chemical warfare** material (green highlighted entries in the yellow or blue bordered pages):

If there is no fire:

- Go directly to Table 1 – Initial Isolation and Protective Action Distances (green-bordered pages).
- Also, consult the assigned guide for the material (orange-bordered pages).

If a fire is involved:

- Go directly to the assigned guide (orange-bordered pages) and apply the distances found under **EVACUATION** - Fire.
- Also, consult Table 1 distances for residual material release.

PROTECTIVE CLOTHING

STREET CLOTHING AND WORK UNIFORMS

These garments, such as uniforms worn by police and emergency medical services personnel, provide almost no protection from the harmful effects of hazardous materials/dangerous goods.

STRUCTURAL FIREFIGHTERS' PROTECTIVE CLOTHING (SFPC)

This category of clothing, often called turnout or bunker gear, is the protective clothing firefighters normally wear during structural firefighting operations. It includes a helmet, coat, pants, boots, gloves and a hood to cover parts of the head that are not protected by the helmet and facepiece. It can be used with full-facepiece positive pressure self-contained breathing apparatus (SCBA). It should, at minimum, meet the OSHA Fire Brigades Standard (29 CFR 1910.156) or NFPA 1851.

Structural firefighters' protective clothing provides limited protection from heat and cold. It may not provide adequate protection from harmful vapors or liquids encountered during hazardous materials/dangerous goods incidents.

Each guide includes a statement about the use of SFPC in incidents involving the materials referenced by that guide. Some guides state that SFPC provides limited protection. In those cases, the responder wearing SFPC and SCBA may be able to perform a quick "in-and-out" operation. However, this type of operation can place the responder at risk of exposure, injury or death. The incident commander makes the decision to do this only if there is an overriding benefit (for example, to perform an immediate rescue, turn off a valve to control a leak, etc.).

Please note that the coverall-type protective clothing customarily worn to fight fires in forests or wildlands is not SFPC and **is not** recommended nor referred to elsewhere in this guidebook.

POSITIVE PRESSURE SELF-CONTAINED BREATHING APPARATUS (SCBA)

This apparatus provides a constant, positive pressure flow of air within the facepiece.

You should always use an SCBA certified by NIOSH and the Department of Labor/Mine Safety and Health Administration, in accordance with:

- 42 CFR Part 84
- requirements for respiratory protection specified in OSHA 29 CFR 1910.134 (Respiratory Protection) and/or 29 CFR 1910.156 (f) (Fire Brigades Standard)
- NFPA 1852

Chemical-cartridge respirators or other filtering masks are not acceptable substitutes for positive pressure SCBA. Demand-type SCBA does not meet the OSHA 29 CFR 1910.156 (f)(1)(i) of the Fire Brigades Standard.

RESPIRATORS

If you suspect a chemical warfare agent is involved in an incident, use NIOSH-certified respirators with CBRN protection.

N95 respirators are the most common of the seven types of particulate filtering facepiece respirators. This product filters at least 95% of airborne particles (0.3 microns), but is not resistant to oil. N95 filtering facepiece respirators do not protect against gases and vapors.

Powered air-purifying respirators (PAPR) force ambient air through the air-purifying cartridge or filter into the facepiece. A PAPR does not supply oxygen or air from a separate source (e.g., cylinders).

CHEMICAL PROTECTIVE CLOTHING AND EQUIPMENT

For you to safely use this type of protective clothing and equipment, you need specific skills developed through training and experience. This type of special clothing may protect against one chemical but be readily permeated by chemicals for which it was not designed. Therefore, do not use this type of protective clothing unless it is compatible with the released material. Also, be aware that it offers little or no protection against heat and/or cold.

Examples of this type of equipment have been described as:

(1) Vapor Protective Suits (NFPA 1991), also known as Totally-Encapsulating Chemical Protective Suits or Level A* protection (OSHA 29 CFR 1910.120, Appendix A & B)

(2) Liquid-Splash Protective Suits (NFPA 1992), also known as Level B* or C* protection (OSHA 29 CFR 1910.120, Appendix A & B), or suits for chemical/biological terrorism incidents (NFPA 1994), class 1, 2 or 3 Ensembles and Standard CAN/CGSB/CSA-Z1610-11 – Protection of first responders from chemical, biological, radiological, and nuclear (CBRN) events

No single protective clothing material will protect you from all hazardous materials/dangerous goods. Do not assume any protective clothing is resistant to cold and/or heat or flame exposure, unless certified by the manufacturer (NFPA 1991 5-3 Flammability Resistance Test and 5-6 Cold Temperature Performance Test).

*Consult the glossary for more information about protection levels under the heading “Protective Clothing.”

DECONTAMINATION

The ways to decontaminate people and equipment can vary. If you need help with decontamination, contact the emergency response telephone number provided on the shipping papers or the agencies listed on the inside back cover. These resources may be able to put you in contact with the chemical manufacturer to determine the appropriate procedure if not otherwise available.

Decontamination is the process of removing or neutralizing hazardous materials/dangerous goods that have contaminated people and equipment during an incident.

Contamination happens in the area generally referred to as the Hot Zone. Everything and everyone entering this zone should be decontaminated when leaving, including emergency response personnel. This reduces the chances that more contamination will occur.

There are two main types of contamination:

- **Direct contamination** happens in the Hot Zone.
- **Cross contamination** happens when someone or something outside the Hot Zone was not properly decontaminated and comes in contact with another object or person, usually in the Warm or Cold Zone.

To decontaminate, you must:

- physically remove contaminants; and/or
- chemically neutralize contaminants*.

The NFPA 472, Chapter 3, describes the following four kinds of decontamination.

(1) **Gross decontamination:** Quickly removing surface contamination, which usually happens by mechanically removing the contaminant or rinsing with water from handheld hose lines, emergency showers, or other nearby water sources.

(2) **Technical decontamination:** Reducing contamination to a level as low as possible by chemical or physical methods. A hazmat team will perform this kind of decontamination.

(3) **Mass decontamination:** Reducing or removing surface contaminants as fast as possible from a large number of people in potentially life-threatening situations.

(4) **Emergency decontamination:** Immediately reducing contamination of people in potentially life-threatening situations with or without formally setting up a decontamination corridor. This process should be performed upwind and uphill from victims. Responders should avoid contact with victims, runoff or spray from the decontamination process.

Emergency and mass decontamination can be done with firefighting and rescue operations equipment. Nozzles can be put on wide-angle fog patterns and sprayed towards the ground to create a decontamination shower. Responders can also place nozzles on the discharge ports of engines.

Contaminated clothing and equipment must be removed after use and stored in a controlled area (Warm Zone) until cleanup procedures can begin. Sometimes protective clothing and equipment cannot be decontaminated and must be disposed of properly.

*Chemical neutralization releases heat. DO NOT PERFORM on a victim.

FIRE CONTROL

Water is the most common and generally most available fire extinguishing agent. Use caution in selecting a fire extinguishing method, as there are many factors to consider. Water may be ineffective in fighting fires that involve some materials.

Fires Involving a Spill of Flammable Liquids

These fires are usually controlled by applying a firefighting foam to the surface of the burning material.

Fighting flammable liquid fires requires:

- foam concentrate that is chemically compatible with the burning material
- correct mixing of the foam concentrate with water and air
- careful application and maintenance of the foam blanket

There are two general types of firefighting foam: regular and alcohol-resistant. Examples of regular foam are protein-base, fluoroprotein, and aqueous film-forming foam (AFFF).

You can control some flammable liquid fires, including many petroleum products, by applying regular foam. Other flammable liquids, including polar solvents (flammable liquids that are water soluble), such as alcohols and ketones, have different chemical properties. You cannot easily control a fire that involves these materials with regular foam, and should use alcohol-resistant foam instead.

Polar solvent fires may be difficult to control and require a higher foam application rate than other flammable liquid fires (see NFPA Standards 11 for further information). Refer to the appropriate guide to determine which type of foam to use. For flammable liquids which have subsidiary corrosive or toxic hazards, it is difficult to make specific recommendations. However, alcohol-resistant foam may be effective for many of these materials.

Contact the emergency response telephone number on the shipping paper, or the appropriate emergency response agency, as soon as possible for guidance on the proper fire extinguishing agent to use.

How you decide to control the fire depends on factors such as:

- incident location
- exposure hazards
- size of the fire
- environmental concerns
- availability of extinguishing agents and equipment at the scene

WATER-REACTIVE MATERIALS

Water is sometimes used to flush spills and reduce or direct vapors in spill situations. Some of the materials covered by this guidebook can react violently or even explosively with water. In these cases, consider letting the fire burn or leaving the spill alone (except to prevent its spreading by diking) until you can get more technical advice.

The applicable guides clearly warn you of these potentially dangerous reactions. Technical advice is required for these materials since:

- Water getting inside a ruptured or leaking container may cause an explosion.
- You may need to cool adjoining containers with water to prevent them from rupturing (exploding), or to prevent the fire spreading further.
- Water may be effective in mitigating an incident involving a water-reactive material, but only if you can apply it at a **sufficient flooding rate for a long period**.
- Products from the reaction with water may be more toxic, corrosive or undesirable than the product that caused the fire.

When you respond to an incident involving water-reactive materials, take into account:

- existing conditions, such as wind, precipitation, location and accessibility to the incident
- availability of agents to control the fire or spill

Because there are variables to consider, base your decision to use water on fires or spills involving water-reactive materials on information from a reliable source. For example, consult the material's manufacturer through the emergency response telephone number or the appropriate emergency response agency listed on the inside back cover.

VAPOR CONTROL

Limiting the amount of vapor released from a pool of flammable or corrosive liquids is an operational concern. It requires proper protective clothing, specialized equipment, appropriate chemical agents and skilled personnel. Before you engage in vapor control, seek advice on tactics to be used from qualified personnel.

There are several ways to minimize the amount of vapors escaping from pools of spilled liquids, such as special foams, adsorbing agents, absorbents, and neutralizing agents. To be effective, you must select a method for the specific material involved, and use it in a way that mitigates, not worsens, the incident.

Where specific materials are known, such as at a manufacturing or storage facilities, the hazardous materials/dangerous goods response team should prearrange with the facility operators to select and stockpile these control agents before a spill.

In the field, first responders may not have the most effective vapor control agent for the material available. They will be more likely to have only water, and only one type of firefighting foam on their vehicles. If the available foam is not appropriate, they will probably use water spray. Because water is being used to form a vapor seal, care must be taken not to churn or further spread the spill during application. Vapors that do not react with water may be directed away from the site using the air currents surrounding the water spray. Before using water spray or other methods to safely control vapor emission or suppress ignition, get technical advice based on a specific chemical name.

BLEVE AND HEAT INDUCED TEAR

BLEVE (BOILING LIQUID EXPANDING VAPOR EXPLOSION)

The following pages present important safety-related information on BLEVEs, including a table, to consider in a situation involving Liquefied Petroleum Gases (LPG), UN1075.

LPGs include the following flammable gases:

- UN1011 - Butane
- UN1012 - Butylene
- UN1055 - Isobutylene
- UN1077 - Propylene
- UN1969 - Isobutane
- UN1978 - Propane

A BLEVE occurs when a fire impinged or damaged tank car fails to contain its internal pressure and explodes with a sudden product release. This catastrophic failure is more likely to occur with damaged pressure tank cars, even in the absence of an active fire.

The **main hazards** from a LPG BLEVE are:

- Fire: If the released substance is ignited, there is an immediate fireball.
- Thermal radiation: At a distance of about 4 times the radius of a fireball, the heat radiated from a fireball is enough to burn exposed skin in 2 seconds. Wearing protective clothing limits the thermal radiation dose.
- Blast: A concussive force caused by the sudden release of the pressurized substance. For a BLEVE occurring out in the open, the blast strength at a distance of 4 times the radius of a fireball can break window glass and may cause minor damage to buildings.
- Projectiles: Tank failure can throw metal fragments over large distances. These fragments can and have been deadly.

The danger decreases as you move away from the BLEVE centre. The furthest-reaching hazard is projectiles.

For a video with information on critical safety issues concerning BLEVEs, please visit *http://www.tc.gc.ca/eng/tdg/publications-menu-1238.html*.

HEAT INDUCED TEAR (HIT)

A heat induced tear (HIT) is a rupture of a NON-PRESSURE tank car containing flammable liquids when exposed to the intense heat of a fire. The metal will soften and the pressure in the tank car will increase which can lead to containment failure. The tear generally occurs at the vapor space (upper side) of the container, venting large quantities of flammable liquid and vapors at high speed. A fireball and an intense heat wave will occur.

Compared to BLEVEs, HITs rarely result in the projection of tank car fragments. Heat induced tearing has occurred within 20 minutes of the derailment and as long as 10+ hours following the initial fire.

Responding to these types of incidents (BLEVE and HIT) requires specialized training, equipment and a tactical approach.

BLEVE – SAFETY PRECAUTIONS

Use with caution. The following table gives a summary of tank properties, critical times, critical distances and cooling water flow rates for various tank sizes. This table is provided to give responders some guidance but it should be used with caution.

Tank dimensions are approximate and can vary depending on the tank design and application.

Minimum time to failure is based on ***severe torch fire impingement*** on the vapor space of a tank in good condition, and is approximate. Tanks may fail earlier if they are damaged or corroded. Tanks may fail minutes or hours later than these minimum times depending on the conditions. It has been assumed here that the tanks are not equipped with thermal barriers or water spray cooling.

Minimum time to empty is based on an engulfing fire with a properly sized pressure relief valve. If the tank is only partially engulfed, then time to empty will increase (i.e., if tank is 50% engulfed, then the tanks will take twice as long to empty). Once again, it has been assumed that the tank is not equipped with a thermal barrier or water spray.

Tanks equipped with thermal barriers or water spray cooling significantly increase the times to failure and the times to empty. A thermal barrier can reduce the heat input to a tank by a factor of ten or more. This means it could take ten times as long to empty the tank through the Pressure Relief Valve (PRV).

Fireball radius and emergency response distance is based on mathematical equations and is approximate. They assume spherical fireballs and this is not always the case.

Two safety distances for public evacuation. The minimum distance is based on tanks that are launched with a small elevation angle (i.e., a few degrees above horizontal). This is most common for horizontal cylinders. The preferred evacuation distance has more margin of safety since it assumes the tanks are launched at a 45 degree angle to the horizontal. This might be more appropriate if a vertical cylinder is involved.

It is understood that these distances are very large and may not be practical in a highly populated area. However, it should be understood that the risks increase rapidly the closer you are to a BLEVE. Keep in mind that the furthest reaching projectiles tend to come off in the zones 45 degrees on each side of the tank ends.

Water flow rate is based on 5 ($\sqrt{\text{capacity (USgal)}}$) = USgal/min needed to cool tank metal.

Warning: the data given are approximate and should only be used with extreme caution. For example, where times are given for tank failure or tank emptying through the pressure relief valve – these times are typical but they can vary from situation to situation. Therefore, never risk life based on these times.

WARNING: The data given are approximate and should only be used with extreme caution. These times can vary from situation to situation. LPG tanks have been known to BLEVE within minutes. Therefore, never risk life based on these times.

BLEVE
(USE WITH CAUTION)

Capacity		Diameter		Length		Propane Mass		Minimum time to failure for severe torch	Approximate time to empty for engulfing fire	Fireball radius		Emergency response distance		Minimum evacuation distance		Preferred evacuation distance		Cooling water flow rate	
Litres	(Gallons)	Meters	(Feet)	Meters	(Feet)	Kilograms	(Pounds)	Minutes	Minutes	Meters	(Feet)	Meters	(Feet)	Meters	(Feet)	Meters	(Feet)	Litres/min	USgal/min
100	(26.4)	0.3	(1)	1.5	(4.9)	40	(88)	4	8	10	(33)	90	(295)	154	(505)	307	(1007)	97	26
400	(106)	0.61	(2)	1.5	(4.9)	160	(353)	4	12	16	(53)	90	(295)	244	(801)	488	(1601)	195	51
2000	(528)	0.96	(3.2)	3	(9.8)	800	(1764)	5	18	28	(92)	111	(364)	417	(1368)	834	(2736)	435	115
4000	(1057)	1	(3.3)	4.9	(16.1)	1600	(3527)	5	20	35	(115)	140	(459)	525	(1722)	1050	(3445)	615	163
8000	(2113)	1.25	(4.1)	6.5	(21.3)	3200	(7055)	6	22	44	(144)	176	(577)	661	(2169)	1323	(4341)	870	230
22000	(5812)	2.1	(6.9)	6.7	(22)	8800	(19400)	7	28	62	(203)	247	(810)	926	(3038)	1852	(6076)	1443	381
42000	(11095)	2.1	(6.9)	11.8	(38.7)	16800	(37037)	7	32	77	(253)	306	(1004)	1149	(3770)	2200	(7218)	1994	527
82000	(21662)	2.75	(9)	13.7	(45)	32800	(72310)	8	40	96	(315)	383	(1257)	1435	(4708)	2200	(7218)	2786	736
140000	(36984)	3.3	(10.8)	17.2	(56.4)	56000	(123457)	9	45	114	(374)	457	(1499)	1715	(5627)	2200	(7218)	3640	962

CRIMINAL OR TERRORIST USE OF CHEMICAL, BIOLOGICAL AND RADIOLOGICAL AGENTS

If you suspect an intentional release of a chemical, biological or radiological agent (CBRN), you should immediately contact your local emergency response authorities (911). Additionally, for CBRN incidents occurring:

- within the United States, call the National Response Center at 1-800-424-8802
- within Canada, call CANUTEC at 613-996-6666 (1-888-226-8832)
- within Mexico, call CENACOM at 555128-0000 extensions 36428, 36422, 36469, 37807, 37810
- in other countries, consult page 392

The following is general guidance and does not serve as specialized incident response training. Do not enter the scene without appropriate training and equipment.

First responders can use the following information to make an initial assessment of a situation they suspect involves criminal or terrorist use of chemical agents, biological agents and/or radioactive materials (CBRN). To help with this, the following paragraphs have a list of observable indicators that a CB agent or radioactive material has been used or is present. This section ends with a Safe Stand-Off Distance Chart for various threats when improvised explosive devices (IEDs) are involved.

DIFFERENCES BETWEEN A CHEMICAL, BIOLOGICAL AND RADIOLOGICAL AGENT

Chemical and biological agents as well as radioactive materials can be dispersed in the air we breathe, the water we drink, or on surfaces we physically contact. Dispersion methods may be as simple as opening a container or using conventional (garden) spray devices, or as elaborate as detonating an improvised explosive device.

Chemical incidents are characterized by the rapid onset of medical symptoms (in minutes to hours) and easily observed signatures (colored residue, dead foliage, pungent odor, dead insects and animals).

Biological incidents are characterized by the onset of symptoms in hours to days. Typically, there will be no characteristic signatures because biological agents are usually odorless and colorless. Because of the delayed onset of symptoms, the affected area may be greater due to the movement of infected people.

Radiological incidents are characterized by the onset of symptoms, if any, in days to weeks or longer. Typically, there will be no characteristic signatures because radioactive materials are usually odorless and colorless. Specialized equipment is needed to determine the size of the affected area, and if the level of radioactivity is an immediate or long-term health hazard. Because it is impossible to detect radioactivity without special equipment, the affected area may be greater due to the migration of contaminated people.

The most probable sources would not generate enough radiation to kill people or cause severe illness. In a radiological incident generated by a "dirty bomb," or radiological dispersal device (RDD), in which a conventional explosive is detonated to spread radioactive contamination, the primary hazard is from the explosion. However, certain radioactive materials dispersed in the air could contaminate up to several city blocks, creating fear and possibly panic, and needing potentially costly cleanup.

INDICATORS OF A POSSIBLE CHEMICAL INCIDENT

Dead animals/birds/fish	Not just an occasional road kill, but numerous animals (wild and domestic, small and large), birds, and fish in the same area.
Lack of insect life	If normal insect activity (ground, air, and/or water) is missing, check the ground, water surface or shore line for dead insects. If near water, check for dead fish and/or aquatic birds.
Unexplained odors	Possible odors include fruity, flowery, sharp, pungent, garlic, horseradish-like, bitter almonds, peach kernels, or newly mown hay. The odor is completely out of character with its surroundings.
Unusual numbers of dying or sick people (mass casualties)	Health problems including nausea, disorientation, difficulty in breathing, convulsions, localized sweating, conjunctivitis (reddening of eyes), erythema (reddening of skin) and death.
Pattern of casualties	Casualties will likely be distributed downwind, or if indoors, by the air ventilation system.
Blisters or rashes	Numerous people experiencing unexplained water-like blisters, weals (like bee stings), and/or rashes.
Illness in confined area	Different casualty rates for people working indoors versus outdoors dependent on where the agent was released.
Unusual liquid droplets	Numerous surfaces show oily droplets or film; numerous water surfaces have an oily film (no recent rain).
Different-looking areas	Not just a patch of dead weeds, but trees, shrubs, bushes, food crops, and/or lawns that are dead, discolored, or withered (no current drought).
Low-lying clouds	Low-lying cloud or fog-like condition not consistent with its surroundings.
Unusual metal debris	Unexplained bomb or munitions-like material, especially if it contains a liquid.

INDICATORS OF A POSSIBLE BIOLOGICAL INCIDENT

Unusual numbers of sick or dying people or animals	Any number of symptoms may occur. Casualties may occur hours to days after an incident has occurred. The time required before symptoms are observed is dependent on the agent.
Unscheduled and unusual spray being disseminated	Especially if outdoors during periods of darkness.
Abandoned spray devices	Devices may not have distinct odors.

INDICATORS OF A POSSIBLE RADIOLOGICAL INCIDENT

Radiation Symbols	Containers may display a “propeller” radiation symbol.
Unusual metal debris	Unexplained bomb or munitions-like material.
Heat-emitting material	Material that is hot or seems to emit heat without any sign of an external heat source.
Glowing material	Strongly radioactive material may emit or cause radioluminescence.
Sick people/animals	In very improbable scenarios there may be unusual numbers of sick or dying people or animals. Casualties may occur hours to days or weeks after an incident has occurred. The time required before symptoms are observed is dependent on the radioactive material used, and the dose received. Possible symptoms include skin reddening or vomiting.

PERSONAL SAFETY CONSIDERATIONS

When you approach a scene that may involve CB agents or radioactive materials, the most critical thing to consider is your safety and that of other responders.

Use protective clothing and respiratory protection of an appropriate level of safety. In incidents where you suspect that CBRN materials have been used as weapons, NIOSH-certified respirators with CBRN protection are highly recommended. Be aware that you may not be able to verify or identify CB agents or radioactive materials, especially in the case of biological or radiological agents.

The following actions apply to a chemical, biological or radiological incident. This guidance is general. Responders will need to apply it on a case-by-case basis.

Approach and response strategies:

- Minimize exposure time.
- Maximize the distance between you and the item that is likely to harm you.
- Use cover as protection.

- Wear appropriate personal protective equipment and respiratory protection.
- Identify and estimate the hazard by using the indicators above.
- Isolate the area and secure the scene.
- Isolate and decontaminate potentially contaminated people as soon as possible.
- To the extent possible, take measures to limit the spread of contamination.

In the event of a **chemical** incident, the fading of chemical odors does not necessarily indicate reduced vapor concentrations. Some chemicals deaden the senses, giving you the false perception that the chemical is no longer present.

If there is any indication that an area may be contaminated with **radioactive** materials, including the site of any non-accidental explosion, responders:

- should be equipped with radiation detection equipment
- should have adequate training in how to use this equipment

This equipment should be designed to also alert responders when an unacceptable ambient dose rate or ambient dose has been reached.

Initial actions to consider in a potential CBRN/terrorism event:

- Avoid using cell phones, radios, etc. within 100 meters (300 feet) of a suspect device.
- Notify your local police by calling 911.
- Set up incident command upwind and uphill of the area.
- Do **not** touch or move suspicious packages or containers.
- Be cautious about the potential presence of secondary devices (e.g., improvised explosive devices (IEDs)).
- Avoid contamination.
- Limit access to only those responsible for rescue of victims or assessment of unknown materials or devices.
- Evacuate and isolate people who were potentially exposed to hazardous materials/ dangerous goods.
- Isolate contaminated areas and secure the scene for analysis of material.

DECONTAMINATION MEASURES

For chemical and biological agents: Emergency responders should follow standard decontamination procedures (flush-strip-flush). Mass casualty decontamination should begin as soon as possible by stripping all clothing, and flushing with soap and water. For further information, contact the agencies listed on the inside back cover of this guidebook.

For people contaminated with radioactive material: Take care to minimize the spread of the contamination to the extent possible. Move them to a low radiation area if necessary, and if it can be done safely. Remove their clothing and place it in a clearly marked and sealed receptacle, such as a plastic bag, for later testing. Use decontamination methods

described above, but avoid breaking the skin (e.g., vigorous brushing). External radiological contamination on intact skin rarely causes a high enough dose to be a hazard, to either the contaminated individual or the first responders. For this reason, prioritize medical stabilization for a contaminated injured individual.

NOTE: The above information was developed in part by the Department of National Defence (Canada), the U.S. Department of the Army, Aberdeen Proving Ground and the Federal Bureau of Investigation (FBI).

IMPROVISED EXPLOSIVE DEVICE (IED)

An IED is a "homemade" bomb and/or destructive device used to destroy, incapacitate, harass, or distract. Because they are improvised, IEDs can come in many forms, ranging from a small pipe bomb to a sophisticated device capable of causing massive damage and loss of life.

The following table predicts the damage radius based on the volume or weight of explosive (TNT equivalent) and the type of bomb.

Improvised Explosive Device (IED)
SAFE STAND-OFF DISTANCE

Threat Description		Explosives Capacity[1]		Mandatory Evacuation Distance[2]		Shelter-in-Place Zone		Preferred Evacuation Distance[3]	
High Explosives (TNT Equivalent)	Pipe Bomb	5 lbs	2.3 kg	70 ft	21 m	71 - 1,199 ft	22 - 365 m	+1,200 ft	366 m
	Suicide Bomber	20 lbs	9 kg	110 ft	34 m	111 - 1,699 ft	35 - 518 m	+1,700 ft	519 m
	Briefcase/Suitcase	50 lbs	23 kg	150 ft	46 m	151 - 1,849 ft	47 - 563 m	+1,850 ft	564 m
	Car	500 lbs	227 kg	320 ft	98 m	321 - 1,899 ft	99 - 579 m	+1,900 ft	580 m
	SUV/Van	1,000 lbs	454 kg	400 ft	122 m	401 - 2,399 ft	123 - 731 m	+2,400 ft	732 m
	Small Delivery Truck	4,000 lbs	1,814 kg	640 ft	195 m	641 - 3,799 ft	196 - 1,158 m	+3,800 ft	1,159 m
	Container/Water Truck	10,000 lbs	4,536 kg	860 ft	263 m	861 - 5,099 ft	264 - 1,554 m	+5,100 ft	1,555 m
	Semi-Trailer	60,000 lbs	27,216 kg	1,570 ft	475 m	1,571 - 9,299 ft	476 - 2,834 m	+9,300 ft	2,835 m

[1] Based on the maximum amount of material that could reasonably fit into a container or vehicle. Variations possible.

[2] Governed by the ability of an unreinforced building to withstand severe damage or collapse.

[3] Governed by the greater of fragment throw distance or glass breakage/falling glass hazard distance. These distances can be reduced for personnel wearing ballistic protection. Note that the pipe bomb, suicide bomb, and briefcase/suitcase bomb are assumed to have a fragmentation characteristic that requires greater stand-off distances than an equal amount of explosives in a vehicle.

Improvised Explosive Device (IED)
SAFE STAND-OFF DISTANCE

Threat Description		LPG Mass / Volume[1]		Fireball Diameter[2]		Safe Distance[3, 4]	
LPG - Butane or Propane	Small LPG Tank	20 lbs / 5 gal	9 kg / 19 L	40 ft	12 m	160 ft	48 m
	Large LPG Tank	100 lbs / 25 gal	45 kg / 95 L	69 ft	21 m	276 ft	84 m
	Commercial/Residential LPG Tank	2,000 lbs / 500 gal	907 kg / 1,893 L	184 ft	56 m	736 ft	224 m
	Small LPG Truck	8,000 lbs / 2,000 gal	3,630 kg / 7,570 L	292 ft	89 m	1,168 ft	356 m
	Semitanker LPG	40,000 lbs / 10,000 gal	18,144 kg / 37,850 L	499 ft	152 m	1,996 ft	608 m

[1] Based on the maximum amount of LPG that could reasonably fit into a container or vehicle. Variations possible.

[2] Assuming efficient mixing of the flammable gas with ambient air.

[3] Determined by U.S. firefighting practices wherein safe distances are approximately 4 times the flame height.

[4] This table is for a loaded LPG tank with explosives on the exterior. Note that an LPG tank filled with high explosives would require a significantly greater stand-off distance than if it were filled with LPG.

GLOSSARY

Adsorbed gas — A gas which sticks (adsorbs) to the surface of a solid and porous material (such as activated charcoal) contained within a metal cylinder. This results in an internal cylinder pressure of less than 101.3 kPa at 20°C (14 psi at 68°F) and less than 300 kPa at 50°C (43 psi at 122°F). These pressures are much lower than those of conventional cylinders containing compressed or liquefied gases.

AEGL(s) — Acute Exposure Guideline Level(s), AEGLs represent threshold exposure limits for the general public after a once-in-a-lifetime, or rare, exposure and are applicable to emergency exposure periods ranging from 10 minutes to 8 hours. Three levels AEGL-1, AEGL-2 and AEGL-3 are developed for each of five exposure periods (10 and 30 minutes, 1 hour, 4 hours, and 8 hours) and are distinguished by varying degrees of severity of toxic effects; see AEGL-1, AEGL-2 and AEGL-3.

AEGL-1 — AEGL-1 is the airborne concentration (expressed as parts per million or milligrams per cubic meter [ppm or mg/m^3]) of a substance above which it is predicted that the general population, including susceptible individuals, could experience notable discomfort, irritation, or certain asymptomatic, non-sensory effects. However, the effects are not disabling and are transient and reversible upon cessation of exposure.

AEGL-2 — AEGL-2 is the airborne concentration (expressed as ppm or mg/m^3) of a substance above which it is predicted that the general population, including susceptible individuals, could experience irreversible or other serious, long-lasting adverse health effects or an impaired ability to escape.

AEGL-3 — AEGL-3 is the airborne concentration (expressed as ppm or mg/m^3) of a substance above which it is predicted that the general population, including susceptible individuals, could experience life-threatening health effects or death.

Alcohol-resistant foam — A foam that is resistant to polar chemicals such as ketones and esters which may break down other types of foam.

Biological agents — Pathogens (bacteria, viruses, etc.) or the toxins they produce (such as anthrax) that are dispersed with criminal intent. They can cause disease or death in otherwise healthy humans. **Refer to GUIDE 158**.

BLEVE — Boiling Liquid Expanding Vapor Explosion

GLOSSARY

Blister agents (vesicants)	Substances that cause blistering of the skin. Exposure is through liquid or vapor contact with any exposed tissue (eyes, skin, lungs). Mustard (H), Distilled Mustard (HD), Nitrogen Mustard (HN) and Lewisite (L) are blister agents. **Symptoms:** Red eyes, skin irritation, burning of skin, blisters, upper respiratory damage, cough, hoarseness.
Blood agents	Substances that injure a person by interfering with cell respiration (the exchange of oxygen and carbon dioxide between blood and tissues). Hydrogen cyanide (AC) and Cyanogen chloride (CK) are blood agents. **Symptoms:** Respiratory distress, headache, unresponsiveness, seizures, coma.
Boil over	A sudden increase in fire intensity associated with the expulsion of burning flammable liquid caused by the boiling of water that has accumulated in the bottom of a tank car.
Burn	Refers to either a chemical or thermal burn, the former may be caused by corrosive substances and the latter by liquefied cryogenic gases, hot molten substances, or flames.
Carcinogen	A substance or mixture which induces cancer or increases its incidence.
Category A	An infectious substance that poses a high risk to the health of individuals and/or animals or public health. These substances can cause serious disease and can lead to death. Effective treatment and preventative measures may not be available.
Category B	An infectious substance that poses a low to moderate risk to individuals and/or animals and/or public health. These substances are unlikely to cause serious disease. Effective treatment and preventative measures are available.
CBRN	Chemical, biological, radiological or nuclear agent.
Choking agents	Substances that cause physical injury to the lungs. Exposure is through inhalation. In extreme cases, membranes swell and lungs become filled with liquid (pulmonary edema). Death results from lack of oxygen; hence, the victim is "choked". Phosgene (CG) is a choking agent. **Symptoms:** Irritation to eyes/nose/throat, respiratory distress, nausea and vomiting, burning of exposed skin.
CO_2	Carbon dioxide gas.

Cold zone Area where the command post and support functions that are necessary to control the incident are located. This is also referred to as the clean zone, green zone or support zone in other documents. (EPA Standard Operating Safety Guidelines, OSHA 29 CFR 1910.120, NFPA 472).

Combustible liquid Liquids which have a flash point greater than 60°C (140°F) and below 93°C (200°F). U.S. regulations permit a flammable liquid with a flash point between 38°C (100°F) and 60°C (140°F) to be reclassed as a combustible liquid.

Compatibility Group Letters identify explosives that are deemed to be compatible. The definition of these Compatibility Groups in this Glossary are intended to be descriptive. Please consult the transportation of hazardous materials/dangerous goods or explosives regulations of your jurisdiction for the exact wording of the definitions. Class 1 materials are considered to be "compatible" if they can be transported together without significantly increasing either the probability of an incident or, for a given quantity, the magnitude of the effects of such an incident.

- A Substances which are expected to mass detonate very soon after fire reaches them.
- B Articles which are expected to mass detonate very soon after fire reaches them.
- C Substances or articles which may be readily ignited and burn violently without necessarily exploding.
- D Substances or articles which may mass detonate (with blast and/or fragment hazard) when exposed to fire.
- E & F Articles which may mass detonate in a fire.
- G Substances and articles which may mass explode and give off smoke or toxic gases.
- H Articles which in a fire may eject hazardous projectiles and dense white smoke.
- J Articles which may mass explode.
- K Articles which in a fire may eject hazardous projectiles and toxic gases.
- L Substances and articles which present a special risk and could be activated by exposure to air or water.

GLOSSARY

Compatibility Group (continued)

N Articles which contain only extremely insensitive detonating substances and demonstrate a negligible probability of accidental ignition or propagation.

S Packaged substances or articles which, if accidentally initiated, produce effects that are usually confined to the immediate vicinity.

Control zones Designated areas at hazardous materials/dangerous goods incidents, based on safety and the degree of hazard. Many terms are used to describe control zones; however, in this guidebook, these zones are defined as the hot/exclusion/red/restricted zone, warm/contamination reduction/yellow/limited access zone, and cold/support/green/clean zone. (EPA Standard Operating Safety Guidelines, OSHA 29 CFR 1910.120, NFPA 472).

Cryogenic liquid A refrigerated, liquefied gas that has a boiling point colder than -90°C (-130°F) at atmospheric pressure or is handled or transported at a temperature equal to or less than -100°C (-148°F).

Decomposition products Products of a chemical or thermal break-down of a substance.

Decontamination The removal of hazardous materials/dangerous goods from personnel and equipment to the extent necessary to prevent potential adverse health effects. See "Decontamination", page 362.

Dry chemical A preparation designed for fighting fires involving flammable liquids, pyrophoric substances and electrical equipment. Common types contain sodium bicarbonate or potassium bicarbonate.

Edema The accumulation of an excessive amount of watery fluid in cells and tissues. Pulmonary edema is an excessive buildup of water in the lungs, for instance, after inhalation of a gas that is corrosive to lung tissue.

ERPG(s) Emergency Response Planning Guideline(s). Values intended to provide estimates of concentration ranges above which one could reasonably anticipate observing adverse health effects; see ERPG-1, ERPG-2 and ERPG-3.

ERPG-1 The maximum airborne concentration below which it is believed nearly all individuals could be exposed for up to 1 hour without experiencing more than mild, transient adverse health effects or without perceiving a clearly defined objectionable odor.

GLOSSARY

ERPG-2 — The maximum airborne concentration below which it is believed nearly all individuals could be exposed for up to 1 hour without experiencing or developing irreversible or other serious health effects or symptoms that could impair an individual's ability to take protective action.

ERPG-3 — The maximum airborne concentration below which it is believed nearly all individuals could be exposed for up to 1 hour without experiencing or developing life-threatening health effects.

Flammable liquid — A liquid that has a flash point of 60°C (140°F) or lower.

Flash point — Lowest temperature at which a liquid or solid gives off vapor in such a concentration that, when the vapor combines with air near the surface of the liquid or solid, a flammable mixture is formed. Hence, the lower the flash point, the more flammable the material.

Flooding quantities — Minimum of 1900 L/min (500 US gal/min) of water.

Hazard zones (Inhalation Hazard Zones)

HAZARD ZONE A: Gases: LC50 of less than or equal to 200 ppm, Liquids: V equal to or greater than 500 LC50 and LC50 less than or equal to 200 ppm.

HAZARD ZONE B: Gases: LC50 greater than 200 ppm and less than or equal to 1000 ppm, Liquids: V equal to or greater than 10 LC50; LC50 less than or equal to 1000 ppm and criteria for Hazard Zone A are not met.

HAZARD ZONE C: LC50 greater than 1000 ppm and less than or equal to 3000 ppm.

HAZARD ZONE D: LC50 greater than 3000 ppm and less than or equal to 5000 ppm.

Please note: even though the term "zone" is used, hazard zones are not an actual area or distance. How zones are assigned is strictly a function of the lethal concentration 50 (LC50) of the product. For example, TIH Zone A is more toxic than Zone D.

High expansion foam — Foams that have a high expansion ratio (over 1:200) with a low water content.

Hot zone — Area immediately surrounding a hazardous materials/dangerous goods incident which extends far enough to prevent adverse effects from the released product to personnel outside the zone. This zone is also referred to as exclusion zone, red zone or restricted zone in other documents. (EPA Standard Operating Safety Guidelines, OSHA 29 CFR 1910.120, NFPA 472).

IED — See "Improvised Explosive Device".

GLOSSARY

Immiscible — In this guidebook, means that a material does not mix readily with water.

Improvised Explosive Device — A bomb that is manufactured from commercial, military or homemade explosives.

Large spill — A spill that involves quantities that are greater than 208 liters (55 US gallons). This usually involves a spill from a large package, or multiple spills from many small packages.

LC50 — Lethal concentration 50. The concentration of a material administered by inhalation that is expected to cause the death of 50% of an experimental animal population within a specified time. (Concentration is reported in either ppm or mg/m^3).

Mass explosion — Explosion which affects almost the entire load virtually instantaneously.

MAWP — Maximum Allowable Working Pressure: The maximum allowable internal pressure that the tank may experience during normal operations.

mg/m^3 — Milligrams of a material per cubic meter of air.

Miscible — In this guidebook, means that a material mixes readily with water.

mL/m^3 — Milliliters of a material per cubic meter of air. (1 mL/m^3 equals 1 ppm).

Mutagen — An agent giving rise to an increased occurrence of mutations in populations of cells and/or organisms. Mutation means a permanent change in the amount or structure of the genetic material in a cell.

Narcotic — A substance which acts as a central nervous system depressor producing effects such as drowsiness, narcosis, reduced alertness, loss of reflexes, lack of coordination, and vertigo. These effects can also be manifested as severe headache or nausea, and can lead to reduced judgment, dizziness, irritability, fatigue, impaired memory function, deficit in perception and coordination, reaction time, or sleepiness.

Nerve agents — Substances that interfere with the central nervous system. Exposure is primarily through contact with the liquid (via skin and eyes) and secondarily through inhalation of the vapor. Tabun (GA), Sarin (GB), Soman (GD) and VX are nerve agents.

Symptoms: Pinpoint pupils, extreme headache, severe tightness in the chest, dyspnea, runny nose, coughing, salivation, unresponsiveness, seizures.

n.o.s. These letters refer to "not otherwise specified". The entries which use this description are generic names such as "Corrosive liquid, n.o.s." This means that the actual chemical name for that corrosive liquid is not listed in the regulations; therefore, a generic name must be used to describe it on shipping papers.

Noxious In this guidebook, means that a material may be harmful or injurious to health or physical well-being.

Organic Peroxide An organic (carbon-containing) compound having two oxygen atoms joined together. Organic peroxides are thermally unstable chemicals. They may have one or more of the following properties: be liable to explosive decomposition; burn rapidly; be sensitive to impact or friction; react dangerously with other substances.

Oxidizer A chemical which supplies its own oxygen and which helps other combustible material burn more readily.

P See "Polymerization".

Packing Group The Packing Group (PG) is assigned based on the degree of danger presented by the hazardous material/dangerous good:

PG I : Great danger
PG II : Medium danger
PG III : Minor danger

PG See "Packing Group".

pH pH is a value that represents the acidity or alkalinity of a water solution. Pure water has a pH of 7. A pH value below 7 indicates an acid solution (a pH of 1 is extremely acidic). A pH above 7 indicates an alkaline solution (a pH of 14 is extremely alkaline). Acids and alkalies (bases) are commonly referred to as corrosive materials.

PIH Poison Inhalation Hazard. See "TIH".

Polar See "Miscible".

Polymerization A chemical reaction that often produces heat and pressure. Once initiated, the reaction is accelerated by the heat that it produces. The uncontrolled buildup of heat and pressure can cause a fire or an explosion, or can rupture closed containers. The letter (**P**) following a guide number in the yellow-bordered and blue-bordered pages identifies a material that may polymerize violently under high temperature conditions or contamination with other products during a transportation incident. It is also used to identify materials that have a strong potential for polymerization in the absence of an inhibitor due to depletion of this inhibitor caused by accident conditions.

ppm Parts per million. (1 ppm equals 1 mL/m^3).

Protective clothing In this guidebook, protective clothing includes both respiratory and physical protection. One cannot assign a level of protection to clothing or respiratory devices separately. These levels were accepted and defined by response organizations such as U.S. Coast Guard, NIOSH, and U.S. EPA.

Level A: SCBA plus totally encapsulating chemical resistant clothing (permeation resistant).

Level B: SCBA plus hooded chemical resistant clothing (splash suit).

Level C: Full or half-face respirator plus hooded chemical resistant clothing (splash suit).

Level D: Coverall, including structural firefighters' protective clothing (SFPC), with no respiratory protection.

SCBA: Self-contained breathing apparatus.

Consult "Protective Clothing", pages 360-361

Pyrophoric A material which ignites spontaneously upon exposure to air (or oxygen).

Radiation Authority As referred to in GUIDES 161 through 166 for radioactive materials, the Radiation Authority is either a Federal, state/provincial agency or state/province designated official. The responsibilities of this authority include evaluating radiological hazard conditions during normal operations and during emergencies. If the identity and telephone number of the authority are not known by emergency responders, or included in the local response plan, the information can be obtained from the agencies listed on the inside back cover. They maintain a periodically updated list of radiation authorities.

Radioactivity The property of some substances to emit invisible and potentially harmful radiation.

Refrigerated liquid See "Refrigerated liquefied gas".

Refrigerated liquefied gas A gas which when packaged for transport is made partially liquid because of its low temperature. See "Cryogenic liquid".

Respiratory sensitizer A substance that induces hypersensitivity of the airways following inhalation of the substance.

Right-of-way A defined area on a property containing one or more high-pressure natural gas pipelines.

Shelter-in-place People should seek shelter inside a building and remain inside until the danger passes. **Sheltering-in-place is used when evacuating the public would cause greater risk than staying where they are, or when an evacuation cannot be performed.** Direct the people inside to **close all doors and windows** and to **shut off all ventilating, heating and cooling systems.** In-place protection (shelter-in-place) may not be the best option if (a) the vapors are flammable; (b) if it will take a long time for the gas to clear the area; or (c) if buildings cannot be closed tightly. Vehicles can offer some protection for a short period if the windows are closed and the ventilating systems are shut off. Vehicles are not as effective as buildings for in-place protection.

Skin corrosion The production of irreversible damage to the skin following the application of a test substance for up to 4 hours.

Skin irritation The production of reversible damage to the skin following the application of a test substance for up to 4 hours.

Skin sensitizer A substance that will induce an allergic response following skin contact.

Small spill A spill that involves quantities that are 208 liters (55 US gallons) or less. This generally corresponds to a spill from a single small package (for example, a drum), a small cylinder, or a small leak from a large package.

Specific gravity Weight of a substance compared to the weight of an equal volume of water at a given temperature. Specific gravity less than 1 indicates a substance is lighter than water; specific gravity greater than 1 indicates a substance is heavier than water.

Straight (solid) stream Method used to apply or distribute water from the end of a hose. The water is delivered under pressure for penetration. In an efficient straight (solid) stream, approximately 90% of the water passes through an imaginary circle 38 cm (15 inches) in diameter at the breaking point. Hose (solid or straight) streams are frequently used to cool tanks and other equipment exposed to flammable liquid fires, or for washing burning spills away from danger points. However, straight streams will cause a spill fire to spread if improperly used or when directed into open containers of flammable and combustible liquids.

TIH Toxic Inhalation Hazard. Term used to describe gases and volatile liquids that are toxic when inhaled (same as PIH). These materials pose a known hazard to human health during transport or is presumed to be toxic to humans because of animal-based studies.

V	Saturated vapor concentration in air of a material in mL/m^3 (ppm) at 20°C and standard atmospheric pressure.
Vapor density	Weight of a volume of pure vapor or gas (with no air present) compared to the weight of an equal volume of dry air at the same temperature and pressure. A vapor density less than 1 (one) indicates that the vapor is lighter than air and will tend to rise. A vapor density greater than 1 (one) indicates that the vapor is heavier than air and may travel along the ground
Vapor pressure	Pressure at which a liquid and its vapor are in equilibrium at a given temperature. Liquids with high vapor pressures evaporate rapidly.
Viscosity	Measure of a liquid's internal resistance to flow. This property is important because it indicates how fast a material will leak out through holes in containers or tanks.
Warm zone	Area between Hot and Cold zones where personnel and equipment decontamination and hot zone support take place. It includes control points for the access corridor and thus assists in reducing the spread of contamination. Also referred to as the contamination reduction corridor (CRC), contamination reduction zone (CRZ), yellow zone or limited access zone in other documents. (EPA Standard Operating Safety Guidelines, OSHA 29 CFR 1910.120, NFPA 472).
Water Reactive Material	In this guidebook, materials which produce significant toxic gas when it comes in contact with water.
Water-sensitive	Substances which may produce flammable and/or toxic decomposition products upon contact with water.

Water spray (fog)

Method or way to apply or distribute water. The water is finely divided to provide for high heat absorption. Water spray patterns can range from about 10 to 90 degrees. Water spray streams can be used to extinguish or control the burning of a fire or to provide exposure protection for personnel, equipment, buildings, etc. **(This method can be used to absorb vapors, knock-down vapors or disperse vapors. Direct a water spray (fog), rather than a straight (solid) stream, into the vapor cloud to accomplish any of the above).**

Water spray is particularly effective on fires of flammable liquids and volatile solids having flash points above 37.8°C (100°F).

Regardless of the above, water spray can be used successfully on flammable liquids with low flash points. The effectiveness depends particularly on the method of application. With proper nozzles, even gasoline spill fires of some types have been extinguished when coordinated hose lines were used to sweep the flames off the surface of the liquid. Furthermore, water spray carefully applied has frequently been used with success in extinguishing fires involving flammable liquids with high flash points (or any viscous liquids) by causing frothing to occur only on the surface, and this foaming action blankets and extinguishes the fire.

PUBLICATION DATA

The 2020 Emergency Response Guidebook (ERG2020) was prepared by the staff of Transport Canada, the U.S. Department of Transportation, and the Secretariat of Communications and Transport of Mexico with the assistance of many interested parties from government and industry including the collaboration of CIQUIME of Argentina. Printing and publication services are provided through U.S. DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA), Outreach, Engagement, and Grants Division.

ERG2020 is based on earlier Transport Canada, U.S. DOT, and Secretariat of Communications and Transport emergency response guidebooks. ERG2020 is published in three languages: English, French and Spanish. The Emergency Response Guidebook has been translated and printed in other languages, including Chinese, German, Hebrew, Japanese, Portuguese, Korean, Hungarian, Polish, Turkish and Thai.

We encourage countries that wish to translate this Guidebook to please contact any of the websites or telephone numbers in the next paragraph.

DISTRIBUTION OF THIS GUIDEBOOK

The primary objective is to place one copy of the ERG2020 in each publicly owned emergency service vehicle through distribution to Federal, state, provincial and local public safety authorities. The distribution of this guidebook is being accomplished through the voluntary cooperation of a network of key agencies. Emergency service organizations that have not yet received copies of ERG2020 should contact the respective distribution center in their country, state or province. In the U.S., information about the distribution center for your location may be obtained from the Office of Hazardous Materials Safety website at https://www.phmsa.dot.gov/hazmat/erg/emergency-response-guidebook-erg or call 202-366-4900. In Canada, contact CANUTEC at 613-992-4624 or via the website at https://www.tc.gc.ca/canutec for information. In Mexico, call SCT at +52 55-57-23-93-00 ext. 20010 or 20577, or via email at cserrano@sct.gob.mx. In Argentina, call CIQUIME at +54-11-5199-1409, or via the website at http://www.ciquime.org or via email at gre@ciquime.org.

REPRODUCTION AND RESALE

Copies of this document which are provided free-of-charge to fire, police and other emergency services may not be resold. ERG2020 (PHH50-ERG2020) may be reproduced without further permission subject to the following:

The names and the seals of the participating governments may not be reproduced on a copy of this document unless that copy accurately reproduces the entire content (text, format, and coloration) of this document without modification. In addition, the publisher's full name and address must be displayed on the outside back cover of each copy, replacing the wording placed on the center of the back cover.

Constructive comments concerning ERG2020 are solicited; in particular, comments concerning its use in handling incidents involving hazardous materials/dangerous goods. Comments should be addressed to:

In Canada:

Director, CANUTEC
Transport Dangerous Goods
Transport Canada
Ottawa, Ontario
Canada K1A 0N5

Phone: 613-992-4624 (information)
Fax: 613-954-5101
Email: canutec@tc.gc.ca

In the U.S.:

U. S. Department of Transportation
Pipeline and Hazardous Materials Safety Administration
Outreach, Engagement, and Grants Division (PHH-50)
Washington, DC 20590-0001

Phone: 202-366-4900
Fax: 202-366-7342
Email: ERGComments@dot.gov

In Mexico:

Secretaría de Comunicaciones y Transportes
Dirección General de Autotransporte Federal
Dirección General Adjunta de Normas y Especificaciones
Técnicas y de Seguridad en el Autotransporte
Calzada de las Bombas No. 411-2 piso,
Col. Los Girasoles,
Alcaldía de Coyoacán,
Código Postal 04920,
Ciudad de México
Phone: +52 55-57-23-93-00 ext. 20010 or 20577
Email: cserrano@sct.gob.mx

In Argentina:

Centro de Información Química para Emergencias (CIQUIME)
Av. Alvarez Thomas 636
C1427CCT Buenos Aires, Argentina
Phone: +54-11-5199-1409
Email: gre@ciquime.org

The Emergency Response Guidebook is normally revised and reissued every four years. However, in the event of a significant mistake, omission or change in the state of knowledge, special instructions to change the guidebook (in pen-and-ink, with paste-over stickers, or with a supplement) may be issued.

Users of this guidebook should check periodically (about every 6 months) to make sure their version is current. Changes should be annotated below. Contact:

DOT/PHMSA
https://www.phmsa.dot.gov/hazmat/erg/emergency-response-guidebook-erg

TRANSPORT CANADA
https://www.tc.gc.ca/eng/canutec/menu.htm

CIQUIME
http://www.ciquime.org

This guidebook incorporates changes dated:

_____

_____

_____

CANADA AND UNITED STATES NATIONAL RESPONSE CENTERS

For the purposes of this guidebook, the terms hazardous materials/dangerous goods are synonymous.

CANADA

1. **CANUTEC**

CANUTEC is the **Canadian Transport Emergency Centre** operated by the Transportation of Dangerous Goods Directorate of Transport Canada.
CANUTEC provides a national bilingual (French and English) advisory service and is staffed by professional scientists experienced and trained in interpreting technical information and providing emergency response advice.

In an emergency, CANUTEC may be called at 1-888-CANUTEC (226-8832)
or collect at 613-996-6666 (24 hours)
***666 cellular (Press Star 666, Canada only)**

In a non-emergency situation, please call the information line at 613-992-4624 (24 hours).

2. PROVINCIAL/TERRITORIAL AGENCIES

Although technical information and emergency response assistance can be obtained from **CANUTEC**, there are federal, provincial and territorial regulations requiring the reporting of dangerous goods incidents to certain authorities.

The following list of provincial/territorial agencies is supplied for your convenience.

Province	Emergency Authority and/or Telephone Number
Alberta	Local Police and Provincial Authorities 1-800-272-9600 or 780-422-9600
British Columbia	Local Police and Provincial Authorities 1-800-663-3456
Manitoba	Provincial Authority 204-945-4888 and Local Police or fire brigade, as appropriate
New Brunswick	Local Police or 1-800-565-1633
Newfoundland and Labrador	Local Police and 709-772-2083
Northwest Territories	867-920-8130
Nova Scotia	Local Police or 1-800-565-1633
Nunavut	Local Police and 867-920-8130
Ontario	Local Police
Prince Edward Island	Local Police or 1-800-565-1633
Quebec	Local Police
Saskatchewan	Local Police or 1-800-667-7525
Yukon Territory	867-667-7244

NOTE:

1. The appropriate federal agency must be notified in the case of rail, air or marine incidents.
2. The nearest police department must be notified in the case of lost, stolen or misplaced explosives, radioactive materials or infectious substances.
3. **CANUTEC must** be notified in the case of:
   a. lost, stolen or unlawfully interfered with dangerous goods (except Class 9)
   b. an incident involving infectious substances
   c. an accidental release from a cylinder that has suffered a catastrophic failure
   d. an incident where the shipping papers display **CANUTEC**'s telephone number 1-888-CANUTEC (226-8832) or 613-996-6666 as the emergency telephone number or
   e. a dangerous goods incident in which a railway vehicle, a ship, an aircraft, an aerodrome or an air cargo facility is involved

3. EMERGENCY RESPONSE ASSISTANCE PLANS (Applies in Canada ONLY)

An ERAP or Emergency Response Assistance Plan is an approved plan that describes what is to be done in the event of a transportation accident involving certain higher risk dangerous goods. The ERAP is required by the Canadian *Transportation of Dangerous Goods Act* for dangerous goods that require special expertise and response equipment to respond to an incident. The plan is intended to assist local emergency responders by providing them with technical experts and specially trained and equipped emergency response personnel at the scene of a dangerous goods incident.

The ERAP will describe the specialized response capabilities, equipment and procedures that will be used to support a response to incidents involving high risk dangerous goods. The plan will also address emergency preparedness, including personnel training, response exercises and equipment maintenance. The ERAP plans supplement those of the carrier and of the local and provincial authorities, and must be integrated with other organizations to help mitigate the consequences of an accident.

For shipments that require an ERAP, the ERAP number and the phone number to activate the ERAP will be included on the shipping paper. If additional information is required, or to determine if the product involved in the emergency requires an ERAP, contact **CANUTEC**.

CANUTEC may be called at 1-888-CANUTEC (226-8832)
or collect at 613-996-6666 (24 hours)
666 on cellular phone (Press star 666) *In Canada Only

NATIONAL RESPONSE CENTER (NRC)

The NRC, which is operated by the U.S. Coast Guard, receives reports required when hazardous materials are spilled. After receiving notification of an incident, the NRC will immediately notify the appropriate Federal On-Scene Coordinator and concerned Federal agencies. Federal law requires that anyone who releases into the environment a reportable quantity of a hazardous material (including oil when water is, or may be affected) or a material identified as a marine pollutant, must **immediately** notify the NRC. When in doubt as to whether the amount released equals the required reporting levels for these materials, the NRC should be notified.

CALL **NRC** (24 hours)

1-800-424-8802

(Toll-free in the U.S., Canada, and the U.S. Virgin Islands)

202-267-2675 in the District of Columbia

Calling the emergency response telephone number, CHEMTREC®, CHEMTEL, INC., INFOTRAC or 3E COMPANY, does not constitute compliance with regulatory requirements to call the NRC.

24-HOUR EMERGENCY RESPONSE TELEPHONE NUMBERS

MEXICO

1. CENACOM

555128-0000 extensions 36428, 36422, 36469, 37807, 37810

2. CONASENUSA

800-11-131-68 in the Republic of Mexico

3. SETIQ

800-00-21-400 or **55-5559-1588**
For calls originating elsewhere, call: **+52-55-5559-1588**

ARGENTINA

1. CIQUIME

0-800-222-2933 in the Republic of Argentina
For calls originating elsewhere, call: **+54-11-4552-8747***

BRAZIL

1. PRÓ-QUÍMICA

0-800-118270 in Brazil
For calls originating elsewhere, call: **+55-19-3833-5310***

COLOMBIA

1. CISPROQUIM

01-800-091-6012 in Colombia
For calls originating in Bogotá, Colombia call: **288-6012**
For calls originating elsewhere call: **+57-1-288-6012**

CHILE

1. CITUC QUÍMICO

2-2247-3600 in the Republic of Chile
For calls originating elsewhere call **+56-2-2247-3600**

* Collect calls are accepted

24-HOUR EMERGENCY RESPONSE TELEPHONE NUMBERS

CANADA

1. CANUTEC

1-888-CANUTEC (226-8832) or **613-996-6666 ***
***666 (STAR 666) cellular** (in Canada only)

UNITED STATES

1. CHEMTREC

1-800-424-9300
(in the U.S., Canada and the U.S. Virgin Islands)
For calls originating elsewhere: **703-527-3887 ***

2. CHEMTEL, INC.

1-888-255-3924
(in the U.S., Canada, Puerto Rico and the U.S. Virgin Islands)
For calls originating elsewhere: **813-248-0573 ***

3. INFOTRAC

1-800-535-5053
(in the U.S., Canada and the U.S. Virgin Islands)
For calls originating elsewhere: **352-323-3500 ***

4. VERISK 3E

1-800-451-8346
(in the U.S., Canada and the U.S. Virgin Islands)
For calls originating elsewhere: **760-602-8703 ***

The emergency response information services shown above maintain periodically updated lists of state and Federal radiation authorities who provide information and technical assistance on handling incidents involving radioactive materials.

5. MILITARY SHIPMENTS, for assistance at incidents involving materials being shipped by, for, or to the Department of Defense (DOD), call one of the following numbers:

703-697-0218 * - Explosives/ammunition incidents
(U.S. Army Operations Center)
1-800-851-8061 - All other hazardous materials/dangerous goods incidents
(Defense Logistics Agency)

6. NATIONWIDE POISON CONTROL CENTER (United States only)
1-800-222-1222

* Collect calls are accepted.

A guidebook intended for use by first responders
during the initial phase of a transportation incident involving hazardous materials/dangerous goods

THIS DOCUMENT SHOULD NOT BE USED TO DETERMINE COMPLIANCE WITH THE HAZARDOUS MATERIALS/ DANGEROUS GOODS REGULATIONS OR TO CREATE WORKER SAFETY DOCUMENTS FOR SPECIFIC CHEMICALS

NOT FOR SALE

This document is intended for distribution free of charge to Public Safety Organizations by the US Department of Transportation and Transport Canada. This copy may not be resold by commercial distributors.

U.S. Department of Transportation
Pipeline and Hazardous Materials Safety Administration
https://www.phmsa.dot.gov/hazmat

Transport Canada Transports Canada
https://www.tc.gc.ca/TDG

SCT
SECRETARÍA DE COMUNICACIONES Y TRANSPORTES
http://www.sct.gob.mx

Employee Performance Evaluation.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

MCSO Employee Performance Evaluation

Employee Name:	CCN:	Employee Job Title:	Rating Period	
			From:	To:

Evaluation Type: (check one) ☐ **Probation** (New Employee/Promotion) ☐ **1st Quarter** ☐ **2nd Quarter** ☐ **3rd Quarter**

☐ **Annual** ☐ **Transfer** ☐ **Other** (specify): _____

Employee Performance Criteria and Measures

Needs Improvement: Performance is clearly below the requirements for the position.

Meets Expectations: Overall performance consistently meets the requirements for the position.

Exceeds Expectations: Overall performance consistently exceeds the expected results of job responsibilities.

PERFORMANCE CRITERIA	Needs Improvement	Meets Expectations	Exceeds Expectations
Appearance: Projects a positive and professional image in grooming, hygiene and dress in accordance with agency standards.			
Initiative: Demonstrates independent action and suggests new ideas to enhance and improve processes; initiates actions to achieve goals beyond what is required.			
Work Performance: Demonstrates knowledge and skills when executing the duties and responsibilities of the position; generates accurate work products; manages work volume.			
Customer Service: Assesses customer needs, provides information or assistance, resolves problems and conducts follow-up and evaluates outcomes.			
Interpersonal Skills: Considers the needs, feelings and capabilities of others; adjusts approaches to respond to different situations; demonstrates cultural competency.			
Critical Thinking/Decision Making: Gathers, interprets and evaluates information using reflective, reasonable, and rational thinking to formulate a decision.			
Safety: Applies safe practices in the performance of duties; including the operation and maintenance of equipment in accordance with departmental standards.			
Planning and Organizing: Coordinates work, sets priorities, and anticipates and determines resource requirements; manages time effectively.			
Policy and Procedures: Demonstrates the required knowledge and compliance level regarding all applicable policies and procedures, state statutes and other related technical knowledge requirements.			

Continued on reverse➔➔

PERFORMANCE CRITERIA	Needs Improvement	Meets Expectations
Attendance and Punctuality: Adheres to the work schedule; consistently punctual; uses leave responsibly; schedules leave appropriately within agency standards.		

Overall Performance Summary: Summarize the employee's overall performance for this period by including explanatory comments consistent with the performance criteria measures. Indicate accomplishments, performance needing improvement, and any actions taken by the employee to improve their performance during this rating period.

Performance Expectations: Cite action-oriented, measurable, specific and time bound future performance expectations related to the employee's job duties and responsibilities:

Career Development: Identify educational, training, and professional development activities for the upcoming evaluation period.

Signatures Below:

This evaluation is based on my observations and knowledge of the employee's performance. Check if documentation is attached: ☐

Evaluator Signature **Date**

I certify that this evaluation was reviewed with me in its completed form and I have received a copy, I understand that I can provide documentation to support my work effort. Check if documentation is attached: ☐

Employee Signature **Date**

I have received this evaluation. It represents facts to the best of my knowledge from observation of both supervisor and employee.

Reviewer Signature **Date**

Division Signature **Date**

Distribution: Original - Human Resources; Copy to Employee; Copy to District/Division/Unit File

Workplace Safety Inspection Checklist.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

WORKPLACE SAFETY INSPECTION CHECKLIST

Completed by: _____ Date: _____

Building: _____ Room: _____

Supervisor: _____ Phone: _____

Department: _____

Scheduled periodic inspections to identify unsafe conditions and work practices are supervisor requirements per Cal OSHA Title 8 CCR 3203(a)(4) and Stanford's Injury and Illness Prevention Program (IIPP). Stanford recommends completing the checklist on an annual basis. Completed copies shall be kept on file for at least one year by the supervisor or department safety coordinator. Report any facility-related deficiencies below to the building manager.

1. GENERAL SAFETY	YES	NO	N/A	COMMENTS/DATE CORRECTED
1. Workplace is clean and orderly.	☐	☐	☐	
2. Floors are clear and aisles, hallways, and exits are unobstructed.	☐	☐	☐	
3. Floor surfaces are kept dry and free of slip hazards.	☐	☐	☐	
4. Stairways, sidewalks, and ramps are free of defects (e.g. damaged treads, frayed carpet).	☐	☐	☐	
5. Illumination is adequate in all common areas and workstations.	☐	☐	☐	
6. Emergency evacuation plans are posted at eye level in every stairway and elevator landing, and immediately inside all public entrances to the building.	☐	☐	☐	
7. All containers, including non-hazardous chemicals and wastes, are labeled with the full chemical or trade name. (For storage of hazardous chemicals, see below*)	☐	☐	☐	
8. Stored materials are secured & limited in height to prevent collapse.	☐	☐	☐	
9. 36" clearance maintained for electrical panels.	☐	☐	☐	
10. Electrical cords and plugs are in good condition with proper grounding.	☐	☐	☐	
11. Extension cords and power strips are not daisy-chained and no permanent extension cords are in use.	☐	☐	☐	
12. Portable electric heaters have at least 36" of clearance from combustible materials (e.g. paper).	☐	☐	☐	
13. Equipment and machines are clean and working properly.	☐	☐	☐	
14. Adequate ventilation is provided to machines for preventing buildup of heat or gas emissions.	☐	☐	☐	
15. Emergency stop switches on machines are identified and in proper working order.	☐	☐	☐	
16. Mechanical safeguards are in place and in proper working order (e.g. paper cutter guards).	☐	☐	☐	

* If chemicals in the work area are stored in amounts greater than typical office/household quantities, you are required to complete the EH&S Laboratory Inspection Checklist quarterly.

SEE NEXT PAGE

2. FIRE	YES	NO	N/A	COMMENTS/DATE CORRECTED
1. Emergency exit signs are properly displayed.	☐	☐	☐	
2. Fire alarms and fire extinguishers are visible and accessible.	☐	☐	☐	
3. Fire doors (e.g. in stairways) are kept closed unless equipped with automatic closing device.	☐	☐	☐	
4. 18" vertical clearance is maintained below all sprinkler heads.	☐	☐	☐	
5. Fire extinguishers are serviced annually.	☐	☐	☐	
6. Corridors and stairways are kept free of obstruction and not used for storage.	☐	☐	☐	
3. EARTHQUAKE	**YES**	**NO**	**N/A**	**COMMENTS/DATE CORRECTED**
1. Bookcases, filing cabinets, shelves, racks, cages, storage cabinets and similar items over four feet tall are anchored to the wall. Refer to ProtectSU for details.	☐	☐	☐	
2. Shelving has lips, bungees or other seismic restraints.	☐	☐	☐	
3. Portable machines or equipment are secured against movement using chains, lockable casters, or other appropriate means.	☐	☐	☐	
4. Top-heavy equipment is bolted down or secured to wall studs to withstand accelerations typically expected in an earthquake.	☐	☐	☐	
5. Large & heavy objects are stored on lower shelves or storage areas.	☐	☐	☐	
6. Valuable equipment sensitive to shock damage, such as instruments, computer disks and glassware are stored in latched cabinets or otherwise secured to prevent falling.	☐	☐	☐	
7. All areas are uncluttered – providing clear evacuation routes in the event of an emergency.	☐	☐	☐	
8. Cabinets and lockers are equipped with positive latching or sliding doors.	☐	☐	☐	

SITE-SPECIFIC INFORMATION/COMMENTS (as needed):

Harrassment and Discrimination Acknowlegment.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

MADISON COUNTY SHERIFF'S OFFICE

ACKNOWLEGMENT OF MADISON COUNTY SHERIFF'S OFFICE HARRASSMENT AND DISCRIMINATION POLICIES

In accordance with the requirements of Section 1001.6.1 of the Madison County Sheriff's Office Discriminatory Harassment Policy, I hereby acknowledge that:

_____ I have had the opportunity to review a copy of the Madison County and Madison County Sheriff's Office Harassment and Discrimination policies.

_____ I understand the Madison County and Madison County Sheriff's Office Harassment and Discrimination policies.

_____ I have had all my questions concerning the Madison County and Madison County Sheriff's Office Harassment and Discrimination policies answered to my satisfaction.

_____ I know how to report alleged harassment and discrimination policy violations.

_____ I have not been the subject of, or witness to, any unreported conduct that may violate the Madison County and Madison County Sheriff's Office Harassment and Discrimination policies.

I hereby affirm that the foregoing statements are true, accurate and complete subject to the penalties provided by MCSO concerning the making of false statements.

_____ _____

Signature of Officer Date

_____

Print Name

_____ _____

Signature of Witness/Supervisor Date

_____

Print Name

Sergeant supplemental Eval.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Madison County Sheriff's Office
Supervisor Supplemental

Development and Training of Subordinates – Is the supervisor consistently developing his/her subordinates thoughtfully and effectively?

Meets Standard	Needs Improvement
☐ Recognizes when a subordinate needs training and ensures the employee receives proper training.	☐ Did not ensure that one or more subordinates received proper training where need for training was clear.
☐ Regularly corrects at-risk behavior of subordinates.	☐ Failed to address at-risk behavior of a subordinate.
☐ Meets occasionally with subordinates to discuss performance expectations, occasionally writes Comment Cards to document employee performance, and monitors employee performance.	☐ Seldom or never meets with subordinates to discuss performance expectations, seldom or never writes Comment Cards to document employee performance, and fails to monitor employee performance.
☐ Regularly reviews and audits RIMS for reports outstanding and insures employees do not fall behind with reports, insures returned reports are completed in a timely manner.	☐ Fails to reviews and audits RIMS for reports outstanding and does insure employees do not fall behind with reports, does not insures returned reports are completed in a timely manner.

Supervisory Administrative Skills – Consider the supervisor's ability to handle the administrative responsibilities associated with the employee's assignment.

Meets Standard	Needs Improvement
☐ Performance evaluations of subordinates accurately reflect performance of subordinates, are generally on time, and are based on real performance and documentation of employees.	☐ Submitted incomplete performance evaluations or granted evaluations that were too generous given the employee's real performance and documentation, or turned in evaluations late.
☐ Completes administrative investigations and reports on time with sufficient information to allow proper action. Investigations and reports require little or no revision.	☐ Submitted reports beyond deadlines, or which were difficult to understand, or which did not fulfill their purpose, or which required repeated kickbacks for substantial revision.

Use of Force and Personnel Complaint Investigation Skills – Consider the ability to manage, investigate, and complete reports for Use of Force incidents and Personnel Complaints.

Meets Standard	Needs Improvement
☐ Responds to and properly manages Categorical and Non-Categorical Use of Force incidents.	☐ Failed to respond to and/or properly manage Categorical or Non-Categorical Use of Force incidents.
☐ Conducts timely and complete Use of Force investigations and associated documentation meeting Department standards.	☐ Submitted Use of Force investigations that were incomplete, required further investigations or revision, inaccurately depicted events or statements, or missed deadlines.
☐ Responds appropriately to public complaint investigations, complaint investigation reports are complete and require minimal kickbacks to make reports effective for making final determinations on findings.	☐ Failed to respond or responded inappropriately to public complaint investigations, produced a complaint investigation report of poor quality, lacking important interviews, missing important addenda, or substantially misparaphrasing interviewee's statement.

Civil Rights Oversight of Field Operations – Ensure that subordinates follow proper procedures in matters of searches, seizures, detentions, arrests, warrants, and related reports.	
Meets Standard	**Needs Improvement**
☐ Properly reviews arrest, booking and charging decisions.	☐ Failed to properly review arrest, booking, and charging decisions.
☐ Properly reviews investigative and arrest reports for detention, probable cause, and search and seizure compliance.	☐ Failed to properly review investigative and arrest reports for detention, probable cause, and search and seizure compliance.
☐ Properly reviews requests for warrants and affidavits to support warrant applications.	☐ Failed to properly reviews requests for warrants and affidavits to support warrant applications.
☐ Properly responds to incidents involving the service of search warrants.	☐ Failed to respond to a search warrant service when a response was required.
☐ Takes affirmative actions to prevent retaliation.	☐ Failed to prevent retaliation when such failure was reasonably avoidable.
☐ Properly evaluates 148 PC arrests for issues regarding training, policy, or tactics.	☐ Failed to properly evaluates 148 PC arrests for issues regarding training, policy, or tactics.
☐ Utilizes and adheres to Department guidelines and procedures regarding the use of confidential information.	☐ Failed to properly utilizes and adheres to Department guidelines and procedures regarding the use of confidential information.

604 Lineup Results Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

LINE-UP FORM

RUNNING THE LINE-UP AND RESULTS

WITNESS:_____ ADMINISTRATOR: _____
(Print Name) *(Print Name)*

Instructions to the administrator conducting the line-up:

- Remain neutral. Do not comment on the identification before, during or after the identification procedure.
- After instructing the witness, stand away and out of the witness' line of sight, while still being able to observe and hear the witness.
- Where practicable and appropriate, video record the entire procedure.
- If video or audio recording obtain consent from the witness.
- A photo should be taken of the line-up and the witness should sign the photo to attest that it represents the line-up that they viewed.
- Introduce by name all individuals present in the viewing room to the witness.
- Tell the witness when the identification procedure will begin, (e.g., "You will now look through the one-way mirror.")
- If there is a need to have a line-up member speak, move, change clothing, or some other activity, then all the line-up members must do the same activity.
- Complete the entire CASE INFORMATION SHEET that accompanies this form.

AFTER THE WITNESS HAS VIEWED THE LINE-UP, ASK THE FOLLOWING QUESTIONS

- Did you recognize anyone in the line-up? _____
- If the answer to the preceding question is negative, STOP and go to the signature line.
- If the answer is positive, proceed to the next question:
- If so, what is the number of the person that you recognize? _____
- From where do you recognize that person? _____

_____

- Record the words and gestures of the witness: _____

_____

CONFIDENCE STATEMENT

In your own words describe your certainty about the choice that you have made. Avoid using numbers. _____

_____

Date: _____ Time: _____ Witness Signature: _____

604 Lineup Case Information Sheet.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

THIS PAGE OF THE FORM **MUST NOT** BE SHOWN TO THE WITNESS

LINE-UP CASE INFORMATION SHEET

Complaint or Case Report #:_____ Crime Date & Location: _____

Line-up Date: _____Time: _____ Location: _____

Crime Committed: _____Witness' Name: _____

Was Witness Transported? Yes □ No □

Transporting Officer: _____

Rank: _____ Command: _____ ID #: _____

Line-up Administrator: _____

Rank: _____ Command: _____ ID #: _____

Investigating Officer: _____

Rank: _____ Command: _____ ID #: _____

Security Officer: _____

Rank: _____ Command: _____ ID #: _____

Asst. District Attorney Present? Yes □ No □

Name of ADA: _____ Phone #: _____

Interpreter Present? Yes □ No □ Name: _____

Was the procedure video recorded? Video Only □ Audio & Video □ Audio Only □ No □

Line-up photograph taken? Yes □ No □ Witness initialed? Yes □ No □

Position	Name	Number Held	Age	Height	Weight
1					
2					
3					
4					
5					
6					

Suspect's name:_____ D.O.B. _____ Position:_____

Comments: _____

_____

Signature of Administrator: _____ Date: _____

1031 Workplace Accident Investigation Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Employee's Report of Injury Form

Instructions: Employees shall use this form to report all work related injuries, illnesses, or "near miss" events (which could have caused an injury or illness) – *no matter how minor*. This helps us to identify and correct hazards before they cause serious injuries. This form shall be completed by employees as soon as possible and given to a supervisor for further action.

I am reporting a work related: ❑ Injury ❑ Illness ❑ Near miss	
Your Name:	
Job title:	
Supervisor:	
Have you told your supervisor about this injury/near miss? ❑ Yes ❑ No	
Date of injury/near miss:	Time of injury/near miss:
Names of witnesses (if any):	
Where, exactly, did it happen?	
What were you doing at the time?	
Describe step by step what led up to the injury/near miss. (continue on the back if necessary):	
What could have been done to prevent this injury/near miss?	
What parts of your body were injured? If a near miss, how could you have been hurt?	
Did you see a doctor about this injury/illness? ❑ Yes ❑ No	
If yes, whom did you see?	Doctor's phone number:
Date:	Time:
Has this part of your body been injured before? ❑ Yes ❑ No	
If yes, when?	Supervisor:
Your signature:	Date:

Supervisor's Accident Investigation Form

Name of Injured Person _____

Date of Birth _____ Telephone Number _____

Address _____

City _____ State_____ Zip _____

(Circle one) Male Female

What part of the body was injured? Describe in detail. _____

_____

What was the nature of the injury? Describe in detail. _____

_____

_____

Describe fully how the accident happened? What was employee doing prior to the event? What equipment, tools being using? _____

_____

_____

Names of all witnesses:

_____ _____

_____ _____

Date of Event _____ Time of Event _____

Exact location of event: _____

What caused the event? _____

_____

_____

Were safety regulations in place and used? If not, what was wrong? _____

_____

Employee went to doctor/hospital? Doctor's Name _____

Hospital Name _____

Recommended preventive action to take in the future to prevent reoccurrence.

_____

_____

_____

_____ _____

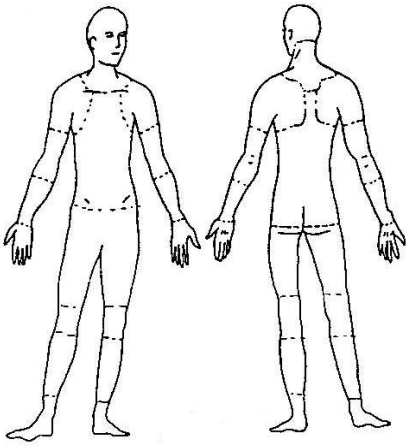
Supervisor Signature Date

Incident Investigation Report

Instructions: Complete this form as soon as possible after an incident that results in serious injury or illness. (Optional: Use to investigate a minor injury or near miss that *could have resulted in a serious injury or illness*.)

This is a report of a: ❑ Death ❑ Lost Time ❑ Dr. Visit Only ❑ First Aid Only ❑ Near Miss	
Date of incident:	This report is made by: ❑ Employee ❑ Supervisor ❑ Team ❑ Other_____

Step 1: Injured employee (complete this part for each injured employee)

Name:	Sex: ❑ Male ❑ Female	Age:
Department:	Job title at time of incident:	
Part of body affected: (shade all that apply) 	Nature of injury: (most serious one) ❑ Abrasion, scrapes ❑ Amputation ❑ Broken bone ❑ Bruise ❑ Burn (heat) ❑ Burn (chemical) ❑ Concussion (to the head) ❑ Crushing Injury ❑ Cut, laceration, puncture ❑ Hernia ❑ Illness ❑ Sprain, strain ❑ Damage to a body system: ❑ Other _____	This employee works: ❑ Regular full time ❑ Regular part time ❑ Seasonal ❑ Temporary Months with this employer Months doing this job:

Step 2: Describe the incident

Exact location of the incident:	Exact time:
What part of employee's workday? ❑ Entering or leaving work ❑ Doing normal work activities ❑ During meal period ❑ During break ❑ Working overtime ❑ Other_____	
Names of witnesses (if any):	

Number of attachments:	Written witness statements:	Photographs:	Maps / drawings:

What personal protective equipment was being used (if any)?

Describe, step-by-step the events that led up to the injury. Include names of any machines, parts, objects, tools, materials and other important details.

Description continued on attached sheets: ❑

Step 3: Why did the incident happen?

Unsafe workplace conditions: (Check all that apply)
- ❑ Inadequate guard
- ❑ Unguarded hazard
- ❑ Safety device is defective
- ❑ Tool or equipment defective
- ❑ Workstation layout is hazardous
- ❑ Unsafe lighting
- ❑ Unsafe ventilation
- ❑ Lack of needed personal protective equipment
- ❑ Lack of appropriate equipment / tools
- ❑ Unsafe clothing
- ❑ No training or insufficient training
- ❑ Other: _____

Unsafe acts by people: (Check all that apply)
- ❑ Operating without permission
- ❑ Operating at unsafe speed
- ❑ Servicing equipment that has power to it
- ❑ Making a safety device inoperative
- ❑ Using defective equipment
- ❑ Using equipment in an unapproved way
- ❑ Unsafe lifting
- ❑ Taking an unsafe position or posture
- ❑ Distraction, teasing, horseplay
- ❑ Failure to wear personal protective equipment
- ❑ Failure to use the available equipment / tools
- ❑ Other: _____

Why did the unsafe conditions exist?

Why did the unsafe acts occur?

Is there a reward (such as "the job can be done more quickly", or "the product is less likely to be damaged") that may have encouraged the unsafe conditions or acts? ❑ Yes ❑ No
If yes, describe:

Were the unsafe acts or conditions reported prior to the incident? ❑ Yes ❑ No

Have there been similar incidents or near misses prior to this one? ❑ Yes ❑ No

Step 4: How can future incidents be prevented?

What changes do you suggest to prevent this incident/near miss from happening again?

❑ Stop this activity ❑ Guard the hazard ❑ Train the employee(s) ❑ Train the supervisor(s)

❑ Redesign task steps ❑ Redesign work station ❑ Write a new policy/rule ❑ Enforce existing policy

❑ Routinely inspect for the hazard ❑ Personal Protective Equipment ❑ Other: _____

What should be (or has been) done to carry out the suggestion(s) checked above?

Description continued on attached sheets: ❑

Step 5: Who completed and reviewed this form? (Please Print)

Written by: Department:	Title: Date:
Names of investigation team members:	
Reviewed by:	Title: Date:

FTO Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Date: **Watch:** **Phase:** **FTO Daily Observation Sheet** **Madison County Sheriff's Office**

Trainee's Last Name	EMP#	FTO's Last Name	EMP #

RATING INSTRUCTIONS: Rate Observed Behavior using the scale below. Comment on the most satisfactory performance of the day. Comment on any behavior that you wish, but a specific comment is required for ratings of "1" or "7". Check the "NO" box if the behavior is not observed. If Trainee fails to respond to training, check "NRT" box, and comment.

RATING

	Not Acceptable FTO Program Standards			Acceptable Level			Superior by FTO Program Standards					
D.S									NO	NRT	**APPEARANCE**	TT
	1	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			1.General Appearance	
											ATTITUDE	
	2	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			2. Acceptance of Feedback	
	3	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			3. Attitude Towards the Job	
											KNOWLEDGE	
											4. Knowledge: Dept Policies and Procedure	
	4	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			Verbal/Written/Simulated Testing	
		1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			Field Performance	
											5. Knowledge of Criminal Statues	
	5	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			Verbal/Written/Simulated Testing	
		1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			Field Performance	
											6. Knowledge of County Ordinances	
	6	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			Verbal/Written/Simulated Testing	
		1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			Field Performance	
											7. Knowledge of Traffic Codes	
	7	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			Verbal/Written/Simulated Testing	
		1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			Field Performance	
											8. Knowledge: Code of Criminal Procedure	
	8	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			Verbal/Written/Simulated Testing	
		1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			Field Performance	
											PERFORMANCE	
	9	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			9.Driving Skill: Normal Conditions	
	10	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			10.Driving Skill:Moderate/High Stress	
	11	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			11.Orientation	
	12	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			12.Routine Forms:Accuracy/Completeness	
	13	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			13. Report Writing: Organization/Detail	
	14	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			14.Report Writing: Grammer/Spelling/Neatness	
	15	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			15.Report Writing: Appropriate Time used	
	16	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			16. Field Performance: Non Stress	
	17	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			17.Field Performance: Stress Conditions	
	18	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			18.Investigative Skill	
	19	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			19.Interview/Interrogation Skill	
	20	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			20.Self-Initiated Field Activity	
	21	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			21.Officer Safety: General	
	22	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			22.Officer Safety:Suspect/Prisoners	
	23	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			23.Control of Conflict: Voice Command	
	24	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			24.Control of Conflict Physical Control	

Date: **Watch:** **Phase:** **FTO Daily Observation Sheet** **Madison County Sheriff's Office**

	25	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			25.Problem Solving/Decision Making	
	26	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			26. Radio: Appropriate Code use	
	27	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			27.Radio: Listens and Comprehends	
	28	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			28. Radio: Articulation of Transmissions	
											RELATIONSHIPS	
	29	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			29: General Public	
	30	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐			30: Ethnic/Cultural/Social Groups	

TOTAL MINUTES OF REMEDIAL TRAINING TIME TODAY (Note Specific Remedial Plan):

The most satisfactory area of performance of the day, was in category number:

A Specific Incident which justifies the rating is:

The least satisfactory performance of the day, was in category number:

A specific incident which justifies the rating is:

CATEGORY #	DOCUMENTATION OF PERFORMANCE AND COMMENTS

WRITE ANY FURTHER COMMENTS ON NARRATIVE CONTINUATION FORM

Trainee's Signature	FTO's Signature
FTO Supervisor's Signature	FTO Coordinator's Signature

1. SET THE STAGE/SCENE 2. CONSIDER VERBATIM QUOTES 3. CRITIQUE PERFORMANCE/NOT THE PERSON
4. USE LISTS AS APPROPRIATE 5. REPORT FACTS/AVOID CONCLUSIONS 6. CHECK SPELLING/GRAMMAR ETC.
7. THINK REMEDIA 8. QUANTIFY WHEN APPROPRIATE 9. REMEMBER YOUR AUDIENCE 10. DON'T PREDICT

Employee Performance Evaluation 2.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

MCSO Employee Performance Evaluation

Employee Name:	**UN:**	**Employee Job Title:**	**Rating Period**	
			From:	**To:**

Evaluation Type: (check one) ☐ **Probation** (New Employee/Promotion) ☐ **1st Quarter** ☐ **2nd Quarter** ☐ **3rd Quarter**

☐ **Annual** ☐ **Transfer** ☐ **Other** (specify): _____

Employee Performance Criteria and Measures

Needs Improvement: Performance is clearly below the requirements for the position.

Meets Expectations: Overall performance consistently meets the requirements for the position.

Exceeds Expectations: Overall performance consistently exceeds the expected results of job responsibilities.

PERFORMANCE CRITERIA	**Needs Improvement**	**Meets Expectations**	**Exceeds Expectations**
Appearance: Projects a positive and professional image in grooming, hygiene and dress in accordance with agency standards.			
Initiative: Demonstrates independent action and suggests new ideas to enhance and improve processes; initiates actions to achieve goals beyond what is required.			
Work Performance: Demonstrates knowledge and skills when executing the duties and responsibilities of the position; generates accurate work products; manages work volume.			
Customer Service: Assesses customer needs, provides information or assistance, resolves problems and conducts follow-up and evaluates outcomes.			
Interpersonal Skills: Considers the needs, feelings and capabilities of others; adjusts approaches to respond to different situations; demonstrates cultural competency.			
Critical Thinking/Decision Making: Gathers, interprets and evaluates information using reflective, reasonable, and rational thinking to formulate a decision.			
Safety: Applies safe practices in the performance of duties; including the operation and maintenance of equipment in accordance with departmental standards.			
Planning and Organizing: Coordinates work, sets priorities, and anticipates and determines resource requirements; manages time effectively.			
Policy and Procedures: Demonstrates the required knowledge and compliance level regarding all applicable policies and procedures, state statutes and other related technical knowledge requirements.			

PERFORMANCE CRITERIA	Needs Improvement	Meets Expectations
Attendance and Punctuality: Adheres to the work schedule; consistently punctual; uses leave responsibly; schedules leave appropriately within agency standards.		

Overall Performance Summary: Summarize the employee's overall performance for this period by including explanatory comments consistent with the performance criteria measures. Indicate accomplishments, performance needing improvement, and any actions taken by the employee to improve their performance during this rating period.

Performance Expectations: Cite action-oriented, measurable, specific and time bound future performance expectations related to the employee's job duties and responsibilities:

Career Development: Identify educational, training, and professional development activities for the upcoming evaluation period.

Signatures Below:

This evaluation is based on my observations and knowledge of the employee's performance. Check if documentation is attached: ☐

Evaluator Signature **Date**

I certify that this evaluation was reviewed with me in its completed form and I have received a copy, I understand that I can provide documentation to support my work effort. Check if documentation is attached: ☐

Employee Signature **Date**

I have received this evaluation. It represents facts to the best of my knowledge from observation of both supervisor and employee.

Reviewer Signature **Date**

Division Signature **Date**

CITAC Business Hours.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

d

r
r

M d r d
rd d

During CITAC hours:

If an individual is in need of an evaluation during CITAC hours, call 540-812-4062 to check availability.

The CITAC is for officer/magistrate initiated ECO's, and for voluntary evaluations accompanied by a law enforcement officer. At this time, we ask that law enforcement remain on scene during the evaluation period. Law enforcement may take an individual to their local ER, but that individual will need to wait until after CITAC hours to be evaluated.

Once at the CITAC the law enforcement officer will sign-in at the front desk, and meet with the security officer and crisis services clinician to go over assessment needs.

If the individual is to be hospitalized under a TDO the transfer of custody form will be completed, and law enforcement will be released to return to service.

If the individual is able to seek outside treatment, the initiating agency will provide transportation back to the individual's residence.

Outside of CITAC hours:

If it is outside of CITAC hours, the individual will be taken to their local medical center ER to be evaluated.

417 Field Training Program Completion Record and Competency Attestation.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Field Training Program Completion Record/ Competency Attestation

REPORT DATE _____

Trainee (Last, First MI)	Badge / ID	Primary Field Training Officer (FTO)	Badge / ID

PART A. PROGRAM COMPLETION

Phase	Field Training Officer	Badge / ID	Shift/Watch	Training Dates (Inclusive)	
1				From:	To:
2				From:	To:
3				From:	To:
4				From:	To:

PART B. TRAINEE ATTESTATION

(ABOVE) WOULD AN ENTIRE PHASE BE DONE IN THE SHIFT/WATCH?

I have been instructed in each phase of the prescribed training contained in the Field Training Program Guide, and my training performance and stages of progress were documented and reviewed with me by training staff as required.

Trainee Signature ▶ _____ **Date**

PART C. TRAINING CERTIFICATION / REQUIRED SIGNATURES

I certify that Officer/Deputy _____ has received the instruction outlined in the Field Training Program Guide and has performed competently in all structured learning content areas. I also certify that all tests have been completed at a satisfactory level and that this trainee is now prepared to work as a solo patrol officer.

Primary FTO Signature ▶ _____ **Date**

Print FT SAC Name	Badge / ID	
		▶ **Date**

PART D. AGENCY HEAD ATTESTATION / REQUIRED SIGNATURES

I attest that the above named trainee has satisfactorily completed the prescribed Field Training Program and is competent to perform as a solo patrol officer.

Print Agency Head Name	Badge / ID	
		▶ **Date**

604 Eyewitness Lineup Instruction Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

LINE-UP FORM

WITNESS INSTRUCTIONS

READ THE FOLLOWING TO THE WITNESS PRIOR TO SHOWING THE LINE-UP:
(Check each box as it is read.)

- ☐ With your consent, the procedure will be recorded using audio, visual or both.
- ☐ Do you consent to recording? ☐ Audio/Video ☐ Audio Only ☐ No Initial: _____
- ☐ As part of our on-going investigation into a crime that occurred at (location) on (date) you are about to view a line-up. (Use similarly neutral language to invite witness to the identification procedure.)
- ☐ You will look through a one-way mirror and see six people in the line-up. They will not be able to see you.
- ☐ There will be a number associated with each person on the other side of the mirror.
- ☐ Take whatever time you want to view the line-up. The perpetrator may or may not be present. You are not required to identify anyone.
- ☐ Do not assume I know who the perpetrator is.
- ☐ I want you to focus on the line-up and not look to me or anyone else in the room for guidance about making an identification during the procedure. Individuals presented in the line-up may not appear exactly as they did at the time of the incident because features, such as head and facial hair, are subject to change.
- ☐ Members of the line-up can be requested to speak, move, or change clothing. If one line-up member is asked to speak, move, or change clothing then all the line-up members will be asked to do the same.
- ☐ If you do make an identification I will ask you to describe your level of certainty about that identification using your own words.
- ☐ After you have had an opportunity to view the line-up I will ask you the following questions:
  1. Do you recognize anyone?
  2. If you do, what is the number of the person you recognize?
  3. From where do you recognize the person?
  4. ONLY IF AN ID IS MADE: In your own words describe your certainty about the choice you have made. Avoid using numbers.
- ☐ I may ask follow up questions.
- ☐ The investigation will continue regardless of whether or not you make an identification.
- ☐ ***DO NOT*** discuss with other witnesses what you see, say or do during this procedure.

I hereby acknowledge that I have read, or have had read to me, the above instructions, and that I understand and will comply with them.

_____ _____

Signature of Witness *Date Signed*

_____

Printed Name of Witness

604 Eyewitness Sequential Photo Lineup Instruction Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

SEQUENTIAL PHOTO ARRAY ID FORM

WITNESS INSTRUCTIONS

READ THE FOLLOWING TO THE WITNESS PRIOR TO SHOWING THE PHOTOS:
(Check each box as it is read.)

- ☐ With your consent, the procedure will be recorded using audio, visual or both.
- ☐ Do you consent to recording? ☐ Audio/Video ☐Audio Only ☐ No Initial: _____
- ☐ As part of our on-going investigation into a crime that occurred at (location) on (date) you are about to view a series of photographs. The person who committed the crime may or may not be included.
- ☐ The photos will be shown to you one at a time and are not in any particular order.
- ☐ There will be a number associated with each person shown in a photo.
- ☐ Take whatever time you want to view the photos. The perpetrator may or may not be present. You are not required to identify anyone. Even if you identify someone during this procedure, I will continue to show you all photos in the series.
- ☐ Do not assume I know who the perpetrator is.
- ☐ I want you to focus on the photographs and not look to me or anyone else in the room for guidance about making an identification during the procedure. Individuals presented in the photos may not appear exactly as they did at the time of the incident because features, such as head and facial hair, are subject to change.
- ☐ If you do make an identification, I will ask you to describe your level of certainty about that identification using your own words.
- ☐ After you have had an opportunity to view the photos, I will ask you the following questions:
  1. Do you recognize anyone?
  2. If you do, what is the number of the person you recognize?
  3. From where do you recognize the person?
  4. ONLY IF AN ID IS MADE: In your own words describe your certainty about the choice you have made. Avoid using numbers.
- ☐ I may ask follow-up questions.
- ☐ The investigation will continue regardless of whether or not you make an identification.
- ☐ ***DO NOT*** discuss with other witnesses what you see, say or do during this procedure.

I hereby acknowledge that I have read, or have had read to me, the above instructions, and that I understand and will comply with them.

_____ _____

Signature of Witness *Date Signed*

_____

Printed Name of Witness

604 Eyewitness Show-up Instruction Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

SHOW-UP FORM

WITNESS INSTRUCTIONS

READ THE FOLLOWING TO THE WITNESS PRIOR TO SHOWING THE SHOW-UP:
(Check each box as it is read.)

- ☐ With your consent, the procedure will be recorded using audio, visual or both.
- ☐ Do you consent to recording? ☐ Audio/Video ☐ Audio Only ☐ No Initials: _____
- ☐ As part of an on-going investigation into a crime that occurred at (location) on (date) you are about to view a show-up of a single individual.
- ☐ Take whatever time you want to view the individual. The individual may or may not be the perpetrator. You are not required to identify anyone. 3.The investigation will continue regardless of whether an identification is made.
- ☐ Do not assume I know who the perpetrator is.
- ☐ I want you to focus on the individual and not look to me or anyone else for guidance about making an identification during the procedure. The Individual presented in the line-up may not appear exactly as did the perpetrator at the time of the incident because features, such as head and facial hair, are subject to change.
- ☐ If you do make an identification, I will ask you to describe your level of certainty about that identification using your own words.
- ☐ After you have had an opportunity to view the individual in the show-up, I will ask you the following questions:

1. Do you recognize the person you viewed?
2. From where do you recognize the person?
3. ONLY IF AN ID IS MADE: In your own words describe your level of certainty about the choice you have made. Avoid using numbers.

- ☐ I may ask follow up questions.
- ☐ The investigation will continue regardless of whether or not you make an identification.
- ☐ ***DO NOT*** discuss with other witnesses what you see, say or do during this procedure.

I hereby acknowledge that I have read, or have had read to me, the above instructions, and that I understand and will comply with them.

_____ _____

Signature of Witness *Date Signed*

_____

Printed Name of Witness

ACCIDENT WITNESS STATEMENT.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Accident Witness Statement

(Please Print – To be completed by Witness – Please return to Supervisor)

ACCIDENT INFORMATION		
Witness's Name:		Witness's Telephone No:
Location where accident occurred:		County Premises: ☐ Yes ☐ No Job Site: ☐ Yes ☐ No
Who was injured:	☐ Employee ☐ Non-Employee	Date of Accident: / / Time of Accident: _____ ☐ am ☐ pm

Describe fully how accident occurred: (including events that occurred immediately before the accident):

Describe bodily injury sustained (be specific about body part(s) affected):

_____ _____

Witness's Signature Date

VA Madison County SO - Victim Witness Agreement.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

COOPERATIVE AGREEMENT

Between
Madison County Victim/Witness Assistance Program
And
Madison County Sheriff's Office
And
Madison County Commonwealth's Attorney's Office
And
Madison County Department of Social Services

The Madison County Sheriff's Office, Madison County Victim/Witness Program, Madison County Commonwealth's Attorney's Office, and Madison County Department of Social Services have agreed to the following measures that will enable these agencies to provide better services to victims of crime. The procedures agreed to herein are intended to ensure that victims of crime will receive information about services available to them and that they are made aware of their rights as victims. These procedures are also designed to encourage the cooperation of victims with law enforcement, prosecution, and the criminal justice process. This agreement broadly defines the services which will be provided by each agency.

1. The Madison County Victim/Witness Program (MCVWP) agrees to the following:

MCVWP will work diligently to contact each victim of violent crime informing them of their rights as crime victims and of the services available to them from MCVWP.

MCVWP will provide services to victims of crime on request of the victim or on referral from MCSO, MCCA or MCDSS.

MCVWP will provide an advocate to MCSO to accompany officers for victim interviews and notifications.

MCVWP will provide training on victims services available upon request from any local agency.

2. The Madison County Sheriff's Office (MCSO) agrees to the following:

MCSO will provide case information crucial to rendering services to victims.

MCSO will assist in the prompt return of property held as evidence.

MCSO officers will make direct referrals to the victim/witness program at their discretion.

3. The Madison County Commonwealth's Attorney's Office (MCCA) agrees to the following:

MCCA will provide the MCVWP with copies of all incident reports and warrants involving victims on a daily basis.

MCCA agrees to honor victim requests to have a support person or victim advocate present during any interview.

MCCA agrees to explain legal alternatives to victims and keep victims informed of any proceedings relevant to their cases.

4. The Madison County Department of Social Services (MCDSS) agrees to the following:

MCDSS agrees to refer victims of crime when appropriate to the MCVWP in a timely manner.

MCDSS agrees to provide updated victim demographical information to MCVWP as appropriate.

When appropriate, MCDSS agrees to provide information to MCVWP in reference to victim interviews, court preparation, and other outside services utilized for the victim.

This agreement is effective April 1, 2021 and will remain in effect until either party terminates in writing. The agreement may be amended, modified or expanded by written mutual agreement of the parties.

Erik J. Weaver
Erik J. Weaver (Mar 8, 2021 14:52 EST)

Erik J. Weaver, Sheriff
Madison County Sheriff's Office

Mar 8, 2021
Date

Clarissa T. Berry

Clarissa T. Berry, Commonwealth's Attorney
Madison County Commonwealth's Attorney's Office

Mar 8, 2021
Date

Valerie Ward
Valerie Ward (Mar 8, 2021 16:28 EST)

Valerie Ward, Director
Madison County Department of Social Services

Mar 8, 2021
Date

Jennifer Hayes
Jennifer Hayes (Mar 8, 2021 16:30 EST)

Jennifer Hayes, Director
Madison County Victim/Witness Program

Mar 8, 2021
Date

Madison County 2020 Co Nurse.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

VACORP

October 2020

MADISON COUNTY
WORKERS' COMPENSATION PANEL OF PHYSICIANS

Herman Stubbe, MD *Rotating Physicians*	**MedExpress Urgent Care 1420 S Main St Culpeper, VA 22701**	540-825-2202
Kristopher Inman, NP V. Veerapalli, MD *Rotating Physicians*	**Culpeper Medical Walk-In Clinic 451 James Madison Hwy Ste 104 Culpeper, VA 22701**	540-727-8880
Michael Silvester, MD Nancy Schmitz, MD Amy Cooley, MD *Rotating Physicians*	**Orange Family Physicians 13198 James Madison Hwy Orange, VA 22960**	540-672-3010

317 Virginia Senior Alert Plan - User Guide.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office



Virginia's

"Senior Alert" Plan

Law Enforcement User's Guide

07-01-07

TABLE OF CONTENTS

	Page
Summary	1
Definitions	1
Statutory Authority	1
Criteria for the Activation of the Plan	2
"Senior Alert" Activation Requirements for All Law Enforcement Agencies	3
Virginia Missing Person Clearinghouse "Senior Alert" Activation Process	4
Virginia " Senior Alert" Activation Flow Chart	5
Appendix A. Virginia "Senior Alert "Agency Request Forms:	
Incident and Agency Contact Information (page 1-2)	6
Authorization to Release of Adult Information (page 3)	8
"Senior Alert" Termination Form	9

SUMMARY

The Virginia "Senior Alert" (VSA) Plan created by legislation in the 2007 General Assembly provides a valuable tool for Virginia law enforcement agencies to help locate missing "senior adults," while allowing the broadcasters of Virginia an opportunity to contribute to the communities they serve. We are hopeful that Virginia's "Senior Alert" Plan will assist in recovering missing Senior Adults who may be in great danger. This plan is available for use by all Virginia law enforcement agencies and can be used as their primary "Senior Alert" Plan or as a supplement to a local plan.

Definitions:

Missing senior adult: an adult whose whereabouts are unknown and who is over 60 years of age and suffers a cognitive impairment to the extent that he is unable to provide care to himself without assistance from a caregiver, including a diagnosis of Alzheimer's Disease or dementia, and whose disappearance poses a credible threat as determined by a law-enforcement agency to the health and safety of the adult and under such other circumstances as deemed appropriate by the Virginia State Police.

Senior alert: the notice of a missing senior adult provided to the public by the media or other methods under a Senior Alert Agreement.

Statutory Authority:

§ 52-34.5. Establishment of the Virginia Senior Alert Program.
The Virginia State Police shall develop policies for the establishment of uniform standards for the creation of Senior Alert Programs throughout the Commonwealth. The Virginia State Police shall (i) inform local law-enforcement officials of the policies and procedures to be used for the Senior Alert Programs; (ii) assist in determining the geographic scope of a particular Senior Alert; and (iii) establish procedures and standards by which a local law-enforcement agency shall verify that a senior adult is missing and shall report such information to the Virginia State Police.
The establishment of a Senior Alert Program by a local law-enforcement agency and the media is voluntary, and nothing in this chapter shall be construed to be a mandate that local officials or the media establish or participate in a Senior Alert Program.

§ 52-34.6. Activation of Senior Alert Program upon an incident of a missing senior adult.
A. Upon receipt of a notice of a missing senior adult from a law-enforcement agency, the Virginia State Police shall confirm the accuracy of the information and provide assistance in the activation of the Senior Alert Program as the investigation dictates.

B. Senior Alerts may be local, regional, or statewide. The initial decision to make a local Senior Alert shall be at the discretion of the local law-enforcement official. Prior to making a local Senior Alert, the local law-enforcement official shall confer with the Virginia State Police and provide information regarding the missing senior adult to the Virginia State Police. The decision to make a regional or statewide Senior Alert shall be at the discretion of the Virginia State Police.

C. The Senior Alert shall include the missing senior adult information as defined in § 15.2-1718.1 and any other such information as the law-enforcement agency deems appropriate that will assist in the safe recovery of the missing senior adult.

D. The Senior Alert shall be cancelled under the terms of the Senior Alert Agreement. Any local law-enforcement agency that locates a missing senior adult who is the subject of an alert shall notify the Virginia State Police immediately that the missing senior adult has been located.

Criteria for the Activation of the Plan

1. **The missing senior adult whereabouts are unknown, is over 60 years of age and;**

2. **Suffers a cognitive impairment to the extent that he or she is unable to provide care for their self without assistance from a caregiver, including a diagnosis of Alzheimer's Disease or dementia, and;**

3. **Whose disappearance poses a credible threat as determined by a law-enforcement agency to the health and safety of the adult and under such other circumstances as deemed appropriate by the Virginia State Police.**

4. **A law enforcement investigation has taken place that verified the senior adult is missing and eliminated alternative explanations by a thorough search of the immediate area if vehicular travel is not involved as a mode of travel for the adult.**

5. **Sufficient information regarding the missing senior adult is available to disseminate to the public that could assist in locating the missing senior adult or their vehicle.**

6. **The missing senior adult must be entered into the Virginia Criminal Information Network (VCIN), the National Crime Information Center (NCIC) missing person files and information reported to the Virginia Missing Person Information Clearinghouse in the prescribed format.**

7. **A photograph of the missing senior adult must be provided to the Virginia Missing Person Information Clearinghouse on the prescribed forms or agency equivalent.**

If all of the aforementioned criteria are not met, the Virginia "Senior Alert" Plan will not be activated however information can still be provided to the media.

"Senior Alert" Requirements for All Law Enforcement Agencies

1. **CONFIRMATION.** Law enforcement agencies are required to confer with the VMPC/State Police prior to activation of a local "Senior Alert". Once the investigating agency has contacted and provided the Virginia Missing Person Information Clearinghouse (VMPC) with the required information, the requesting agency will only be required to submit updated information and notify the VMPC of the recovery of the missing senior adult or cancellation of the alert.

2. **INVESTIGATION POLICY**
    a. AGENCY POLICY. Agencies must follow their intra-departmental policy regarding the actual investigation process involving missing person incidents within their jurisdiction.
    b. ACTIVE. An investigation must be ongoing and active prior to requesting the Virginia Senior Alert activation.
    c. VCIN/NCIC. The agency must have entered the missing person into the VCIN/NCIC systems.

3. **POINT OF CONTACT.** The agency must designate at least one officer as a point of contact for the VMPC to communicate with during the incident.

4. **PHONE CAPABILITY**
    a. The agency must have an assigned telephone number capable of rolling over to at least two separate lines to take telephone calls if the Virginia "Senior Alert" Plan is activated, or have made arrangements with the Virginia Missing Person Information Clearinghouse to take the telephone calls and forward the information to the law enforcement agency.
    b. The agency must have volunteers or personnel to receive telephone calls for a minimum of 24-hours or until the alert is canceled, or have made arrangements with the Virginia Missing Person Information Clearinghouse to handle these duties.

5. **NECESSARY INFORMATION.** Upon activation of the agency's or Virginia's "Senior Alert" Plan, the following information must be immediately submitted to the Virginia Missing Children Information Clearinghouse:
    a. A photograph of the missing person.
    b. Required information listed in the Virginia "Senior Alert" Activation forms or Agency form, and as set forth in the Virginia "Senior Alert" Plan.
    c. Updated information regarding the case. The VMPC will disseminate the pertinent information to participating television and radio stations.
    d. Immediate notification that the missing "senior adult" has been located, or upon closure of the case. The VMPC will notify all components of the Virginia "Senior Alert" (VSA) Plan regarding the termination of the VSA.

6. **TERMINATION.** Agencies must notify VMPC using the appropriate form if the investigation is terminated within 12 hours.

7. **SP-67 FORM.** The Agency must submit the completed SP-67 or equivalent agency form.

VMPC "SENIOR ALERT" ACTIVATION PROCESS

Activation of the Virginia "Senior Alert" Plan must be initiated through the Virginia State Police VMPC. Once the agency receives a report that meets the established age criteria, the following process shall be followed:

1. Complete the included pre-established Virginia "Senior Alert" form packet and forward to the Virginia Missing Person Information Clearinghouse.

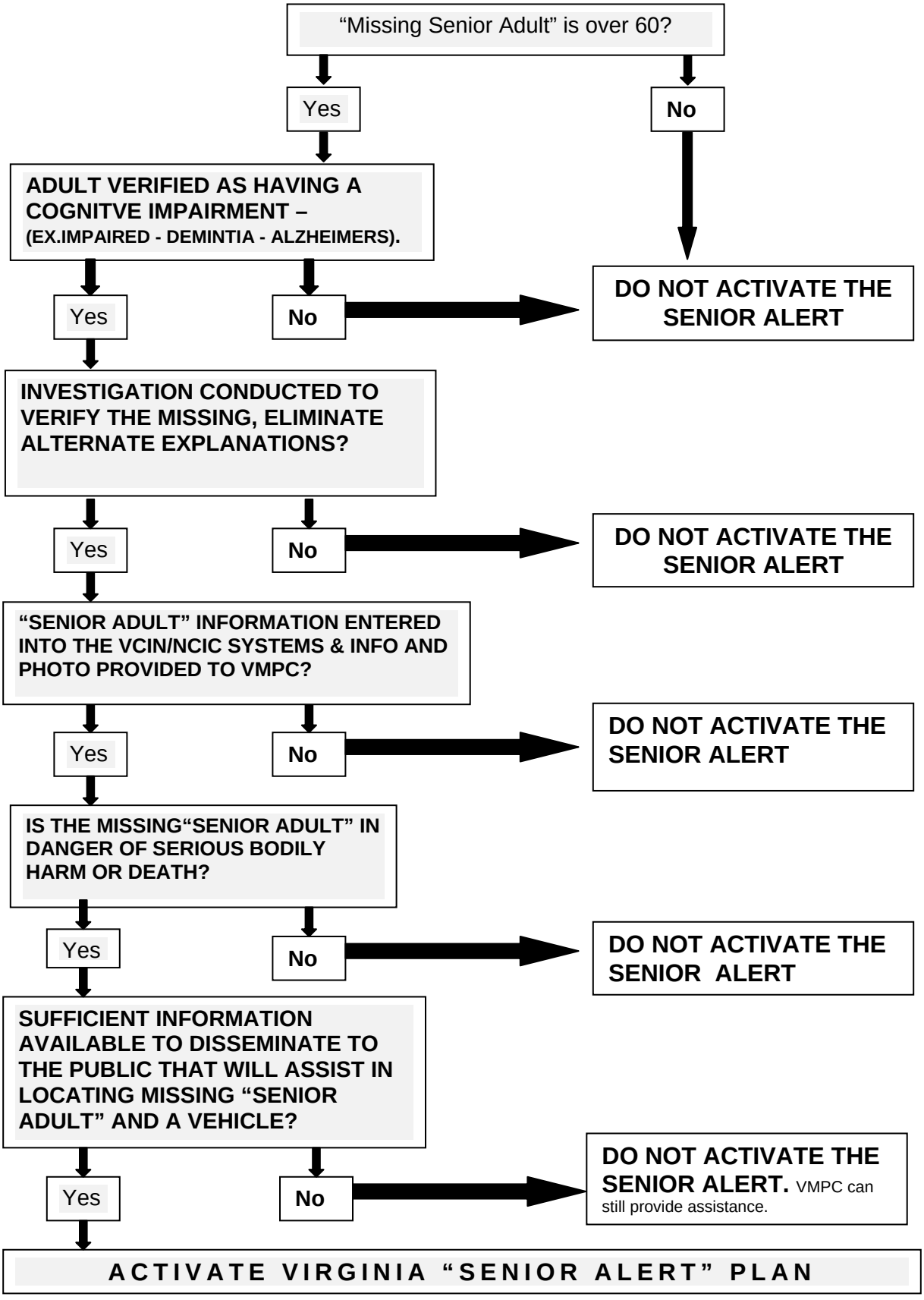
2. Notify VMPC by telephone and immediately confirm our receipt of the packet information. If you should have any difficulties transmitting information, designate a department contact for VMPC (include a name and telephone number on the standardized facsimile form).

3. Forward the most current photograph of the missing "senior adult" immediately and forward all incident details or summaries to the Virginia Missing Person Information Clearinghouse dutysgthq@vsp.virginia.gov. The electronic image of the photograph must be in Joint Photographic Experts Group (JPEG) format.

   Telephone #: 804-674-2026 Forms only - Facsimile #: 804-674-6704

4. The Virginia State Police will contact any/all broadcasting companies through email and facsimile message upon approval to activate the Virginia "Senior Alert" Plan" The Virginia State Police will provide supplemental information by email and facsimile with a detailed summary of the missing "senior adult", and forward a copy of their photograph to any/all broadcasting companies.

DECISION FLOWCHART FOR VIRGINIA "SENIOR ALERT" PLAN ACTIVATION



APPENDIX A

VIRGINIA “SENIOR ALERT” AGENCY REQUEST FORMS

Virginia "Senior Alert" Agency Request Form

Incident Information

Date Missing: _____ **Time Reported Missing:** _____
(mm/dd/yy) (hh:mm)

Location of Incident - last known location:
_____
(Description)

Direction of Travel/Destination: _____
(City, State, Subdivision)

Vehicle Description: _____
(Make, Model, Year, Color, License Plate Number and State of Issue)

Missing "Senior Adult" (Complete an additional page for each adult reported missing)

Name: _____
(Last, First, MI)

Gender: _____ **DOB:** _____ **Race:** _____
(Male/Female) (mm/dd/yy or Approx. Year) (Include all Types)

Height: _____ **Weight:** _____ **Hair**_____ **Eyes:** _____
(Feet/Inches) (Lbs.) (Style and Color) (Color)

Clothing:

Shirt: _____
(Type, Long or Short Sleeve, Color)

Pants: _____
(Type and Color)

Shoes: _____
(Type and Color)

Other: _____
(Type and Color)

Outerwear: _____
(Type and Color)

Additional Significant Identifiers:_____
_____

Medical Needs: _____

OBTAIN A PHOTOGRAPH OF THE MISSING SENIOR ADULT, AND E-MAIL TO THE VIRGINIA MISSING PERSON INFORMATION CLEARINGHOUSE
dutysgthq@vsp.virginia.gov

Details:_____
_____

Virginia "Senior Alert" Agency Request Form

Page 2

CONTACT ORGANIZATION:

Sheriff's Office or Police Department: _____

Contact Person:_____

Telephone Number:_____ **Facsimile Number:** _____

Pager Number: _____ **Cellular Telephone Number:** _____

Date and Time Submitted: _____

Virginia "Senior Alert" Agency Request Form

AUTHORIZATION FOR RELEASE OF ADULT INFORMATION

For a period of one year from the execution of this form, the undersigned authorizes full disclosure of all records concerning the missing adult to any agent of the state of Virginia, Virginia State Police, or any individual or entity assigned by the Virginia State Police, whether the records are of a public, private, internal, or confidential nature. I direct the release of such information regardless of any agreement I may have made to the contrary with any entity or individual to whom the missing adult's information is released or presented. The intent of this authorization is to give my consent for full and complete disclosure of potentially confidential information. Additionally, I understand the duty of the Virginia State Police to release any information to the proper authorities and make other reports as may be mandated by law. I also certify that any person(s) who may furnish such information concerning the missing adult shall not be held accountable for giving this information; and I do hereby release such person(s) from any and all liability which may be incurred as a result of furnishing such information. I further release the Virginia State Police, Virginia Broadcasters Association and its agents, and designees under this release, from any and all liability which may be incurred as a result of furnishing such information. A photocopy of this release form will be valid as an original thereof, even though the said photocopy does not contain an original writing of my signature. I have read and fully understand the contents of this "Authorization for Release of Information."

PLEASE PRINT OR TYPE:

_____

Last Name, First Name, Middle Initial

_____

Current Address, House Number/Box Number Street Name/Rural Route, City, State, Zip Code

Signature : _____

LIABILITY AGREEMENT:

I hereby agree the information I have provided to you acting as an agent of the state of Virginia, Virginia State Police, Virginia Broadcasters Association or any individual or entity assigned by the Virginia State Police, to be truthful, factual, and correct. As the guardian or caregiver for the missing adult, I am aware that in order for the Virginia State Police to activate the Virginia "Senior Alert," the following criteria must be met:

1. The missing senior adult is 60 years of age or older, and
2. The guardian/caregiver ***must reasonably believe*** the missing senior adult has a cognitive impairment, dementia or Alzheimer's and ***is in danger*** of serious bodily harm or death.

I am also aware I may be charged criminally for committing the crime of knowingly providing false information to law enforcement authorities. I have read and fully understand the contents of this "Liability Agreement."

PLEASE PRINT OR TYPE:

_____

Last Name, First Name, Middle Initial

_____

Current Address, House Number/Box Number Street Name/Rural Route, City, State, Zip Code

Signature : _____

Virginia "SENIOR" Termination Form

We are terminating the "Senior Alert" originated by our agency. Please broadcast the following information as necessary.

Text Follows

The "Senior Alert" which was transmitted earlier for

(*Full name*)_____, missing from

(*Street*) _____ in

(*City or County*) _____, has been

canceled. The "Senior Alert" for (*Full name*)_____

_____has been canceled.

Text Ends

Originating Agency: _____

317 Virginia Senior Alert Request Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Virginia "Senior Alert" Request Form

Incident Information

Date Missing: _____ (mm/dd/yy) **Time Reported Missing:** _____ (hh:mm)

Location of Incident - last known location:

_____
(Description)

Direction of Travel/Destination:

_____
(City, State, Subdivision)

Vehicle Description:

_____
(Make, Model, Year, Color, License Plate Number and State of Issue)

Missing "Senior Adult" (Complete an additional page for each adult reported missing)

Name: _____
(Last, First, MI)

Gender: _____ (Male/Female) **DOB:** _____ (mm/dd/yy or Approx. Year) **Race:** _____ (Include all Types)

Height: _____ (Feet/Inches) **Weight:** _____ (Lbs.) **Hair:** _____ (Style and Color) **Eyes:** _____ (Color)

Clothing:

Shirt: _____
(Type, Long or Short Sleeve, Color)

Pants: _____
(Type and Color)

Shoes: _____
(Type and Color)

Other: _____
(Type and Color)

Outerwear: _____
(Type and Color)

Additional Significant Identifiers: _____

_____

Medical Needs: _____

OBTAIN A PHOTOGRAPH OF THE MISSING SENIOR ADULT, AND E-MAIL TO THE VIRGINIA MISSING PERSON INFORMATION CLEARINGHOUSE dutysgthq@vsp.virginia.gov.

Details: _____

_____

Virginia "Senior Alert" Request Form

CONTACT ORGANIZATION:

Sheriff's Office or Police Department: _____

Contact Person: _____

Telephone Number: _____ **Facsimile Number:** _____

Pager Number: _____ **Cellular Telephone Number:** _____

Date and Time Submitted: _____

Virginia "Senior Alert" Agency Request Form

AUTHORIZATION FOR RELEASE OF ADULT INFORMATION

For a period of one year from the execution of this form, the undersigned authorizes full disclosure of all records concerning the missing adult to any agent of the state of Virginia, Virginia State Police, or any individual or entity assigned by the Virginia State Police, whether the records are of a public, private, internal, or confidential nature. I direct the release of such information regardless of any agreement I may have made to the contrary with any entity or individual to whom the missing adult's information is released or presented. The intent of this authorization is to give my consent for full and complete disclosure of potentially confidential information. Additionally, I understand the duty of the Virginia State Police to release any information to the proper authorities and make other reports as may be mandated by law. I also certify that any person(s) who may furnish such information concerning the missing adult shall not be held accountable for giving this information; and I do hereby release such person(s) from any and all liability which may be incurred as a result of furnishing such information. I further release the Virginia State Police, Virginia Broadcasters Association and its agents, and designees under this release, from any and all liability which may be incurred as a result of furnishing such information. A photocopy of this release form will be valid as an original thereof, even though the said photocopy does not contain an original writing of my signature. I have read and fully understand the contents of this "Authorization for Release of Information."

PLEASE PRINT OR TYPE:

Last Name, First Name, Middle Initial

Current Address, House Number/Box Number Street Name/Rural Route, City, State, Zip Code

Signature _____

LIABILITY AGREEMENT:
I hereby agree the information I have provided to you acting as an agent of the state of Virginia, Virginia State Police, Virginia Broadcasters Association or any individual or entity assigned by the Virginia State Police, to be truthful, factual, and correct. As the guardian or caregiver for the missing adult, I am aware that in order for the Virginia State Police to activate the Virginia "Senior Alert," the following criteria must be met:

1. The missing senior adult is 60 years of age or older, and
2. The guardian/caregiver ***must reasonably believe*** the missing senior adult has a cognitive impairment, dementia or Alzheimer's and ***is in danger*** of serious bodily harm or death.

I am also aware I may be charged criminally for committing the crime of knowingly providing false information to law enforcement authorities. I have read and fully understand the contents of this "Liability Agreement."

PLEASE PRINT OR TYPE:

Last Name, First Name, Middle Initial

Current Address, House Number/Box Number Street Name/Rural Route, City, State, Zip Code

Signature: _____

317 Virginia Missing Child With Autism Alert Plan User Guide.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

VIRGINIA

MISSING PERSON WITH AUTISM ALERT PLAN

APPROVED BY: Gary T. Settle DATE: 6-25-21

Colonel Gary T. Settle
Superintendent

TABLE OF CONTENTS

	Page
Summary	1
Definitions	1
Statutory Authority	2
Criteria for the Activation of the Plan	3
Activation Requirements for All Law Enforcement Agencies	4
Virginia Missing Person Clearinghouse “Missing Person with Autism” Alert Activation Process	5
Virginia “Missing Person with Autism” Activation Flow Chart	6
Appendix A. Virginia Missing Person with Autism Alert Forms:	7
Agency Request for Activation of alert (page 1-2)	8-9
Authorization for Release of Information form (page 3)	10
Request for Termination of Alert form	11

SUMMARY

The Virginia Missing Person with Autism Alert Plan created by legislation in the 2021 provides a valuable tool for Virginia law enforcement agencies to help locate missing Person with Autism, while allowing the broadcaster of Virginia an opportunity to contribute to the communities they serve. We are hopeful that Virginia's Missing Person with Autism Alert Plan will assist in recovering missing Autistic Persons who may be in great danger. This plan is available for use by all Virginia law enforcement agencies and can be used as their primary Missing Person with Autism Alert Plan or as a supplement to a local plan.

Definitions:

*§ **52-34.13**. Definitions.*

"Media" means print, radio, television, and Internet-based communication systems or other methods of communicating information to the public.

*"Missing person with autism" means any person (i) whose whereabouts are unknown; (ii) who has been diagnosed with autism spectrum disorder as defined in § **38.2-3418.17**; and (iii) whose disappearance poses a credible threat as determined by law enforcement to the safety and health of the person and under such other circumstances as deemed appropriate by the Virginia State Police.*

"Missing person with Autism Alert" means the notice of a missing person with autism provided to the public by the media or other methods under a Missing Person with Autism Alert Agreement.

"Missing Person with Autism Alert Agreement" means a voluntary agreement between law-enforcement officials and members of the media whereby a person with autism will be declared missing, and the public will be notified by media outlets, and includes all other incidental conditions of the partnership as found appropriate by the Virginia State Police.

"Virginia Missing Person with Autism Alert Program" or "Program" means the procedures and Missing Person with Autism Alert Agreements to aid in the identification and location of a missing person with autism.

Statutory Authority:

§ 52-34.14. Establishment of the Virginia Missing Person with Autism Alert Program.

The Virginia State Police shall develop policies for the establishment of uniform standards for the creation of Virginia Missing Person with Autism Alert Programs throughout the Commonwealth. The Virginia State Police shall (i) inform local law-enforcement officials of the policies and procedures to be used for the Missing Person with Autism Alert Programs; (ii) assist in determining the geographic scope of a particular Missing Person with Autism Alert; and (iii) establish procedures and standards by which a local law-enforcement agency shall verify that a person with autism is missing and shall report such information to the Virginia State Police.

The establishment of a Missing Person with Autism Alert Program by a local law-enforcement agency and the media is voluntary, and nothing in this chapter shall be construed to be a mandate that local officials or the media establish or participate in a Missing Person with Autism Alert Program.

§ 52-34.15. Activation of Virginia Missing Person with Autism Alert Program upon incident of a missing person with autism.

A. Upon receipt of a notice of a missing person with autism from a law-enforcement agency, the Virginia State Police shall confirm the accuracy of the information and provide assistance in the activation of the Missing Person with Autism Alert Program as the investigation dictates.

B. Missing Person with Autism Alerts may be local, regional, or statewide. The initial decision to make a local Missing Person with Autism Alert shall be at the discretion of the local law-enforcement official. Prior to making a local Missing Person with Autism Alert, the local law-enforcement official shall confer with the Virginia State Police and provide information regarding the missing person with autism to the Virginia State Police. The decision to make a regional or statewide Missing Person with Autism Alert shall be at the discretion of the Virginia State Police.

C. The Missing Person with Autism Alert shall include such information as the law-enforcement agency deems appropriate that will assist in the safe recovery of the missing person with autism.

D. The Missing Person with Autism Alert shall be canceled under the terms of the Missing Person with Autism Alert Agreement. Any local law-enforcement agency that locates a missing person with autism who is the subject of an alert shall notify the Virginia State Police immediately that the missing person with autism has been located.

Criteria for the Activation of the Plan

1. The missing persons whereabouts are unknown, and;

2. Has been diagnosed with autism spectrum disorder and;

3. Whose disappearance poses a credible threat as determined by law enforcement to the safety and health of the person and under such other circumstances as deemed appropriate by the Virginia State Police.

4. A law enforcement investigation has taken place that verified the person is missing and eliminated alternative explanations by a thorough search of the immediate area if vehicular travel is not involved as a mode of travel.

5. Sufficient information regarding the missing person is available to disseminate to the public that could assist in locating the missing person.

6. The missing person must be entered into the Virginia Criminal Information Network (VCIN), the National Crime Information Center (NCIC) missing person files and information reported to the Virginia Missing Person Clearinghouse (VMPC) in the prescribe format.

If all of the aforementioned criteria are not met, the Virginia Missing Person with Autism Alert Plan will not be activated however information can still be provided to the media.

Missing Person with Autism Alert Requirements for All Law Enforcement Agencies

1. **CONFORMATION.** Law enforcement agencies are required to confer with the VMPC/State Police prior to activation of a local "Missing Person with Autism Alert". Once the investigating agency has contacted and provided the Virginia Missing Person Clearinghouse (VMPC) with the required information, the requesting agency will only be required to submit updated information and notify the VMPC of the recovery of the missing person or cancellation of the alert.
2. **INVESTIGATION POLICY.**
    - **a.** AGENCY POLICY. Agencies must follow their intra-departmental policy regarding the actual investigation process involving missing person incidents within their jurisdiction.
    - **b.** ACTIVE. An investigation must be ongoing and active prior to requesting the Missing Person with Autism Alert activation.
    - **c.** VCIN/NCIC. The agency must have entered the missing person into the VCIN/NCIC systems.
3. **POINT OF CONTACT.** The agency must designate at least one officer as a point of contact for the VMPC to communicate with during the incident.
4. **PHONE CAPABILITY**
    a. The agency must have an assigned telephone number capable of rolling over to at least two separate lines to take telephone calls if the Missing Person with Autism Alert Plan is activated, or have made arrangements with the Virginia Missing Person Clearinghouse to take the telephone calls and forward the information to the law enforcement agency.

5. **NECESSARY INFORMATION.** Upon activation of the agency's or Virginia's "Missing Person with Autism Alert" Plan, the following information must be immediately submitted to the Virginia Missing Person Clearinghouse:
    a. A photograph of the missing person.
    b. Required information listed in the Virginia Missing Person with Autism Alert Activation forms or Agency form and as set forth in the Virginia Missing Person with Autism Alert Plan.
    c. Updated information regarding the case. The VMPC will disseminate the pertinent information to participating television and radio stations.
    d. Immediate notification that the missing person has been located, or upon closure of the case. The VMPC will notify all components of the Virginia Missing Person with Autism Alert Plan regarding the termination of the alert.

6. **TERMINATION.** Agencies must notify VMPC using the appropriate form if the investigation is terminated within 12 hours.
7. **SP-183 or SP-67 FORM.** Depending on the missing person's age, the agency must submit either a completed SP-183 (Child) or the SP-67 (Adult) or equivalent agency form.

VMPC Missing Person with Autism Alert ACTIVATION PROCESS

Activation of the Virginia Missing Person with Autism Alert Plan must be initiated through the Virginia State Police. Once the agency receives a report that meets the established age criteria,

1. Complete the included pre-established Virginia Missing Person with Autism Alert form packet and forward to the Virginia Missing Person Information Clearinghouse.

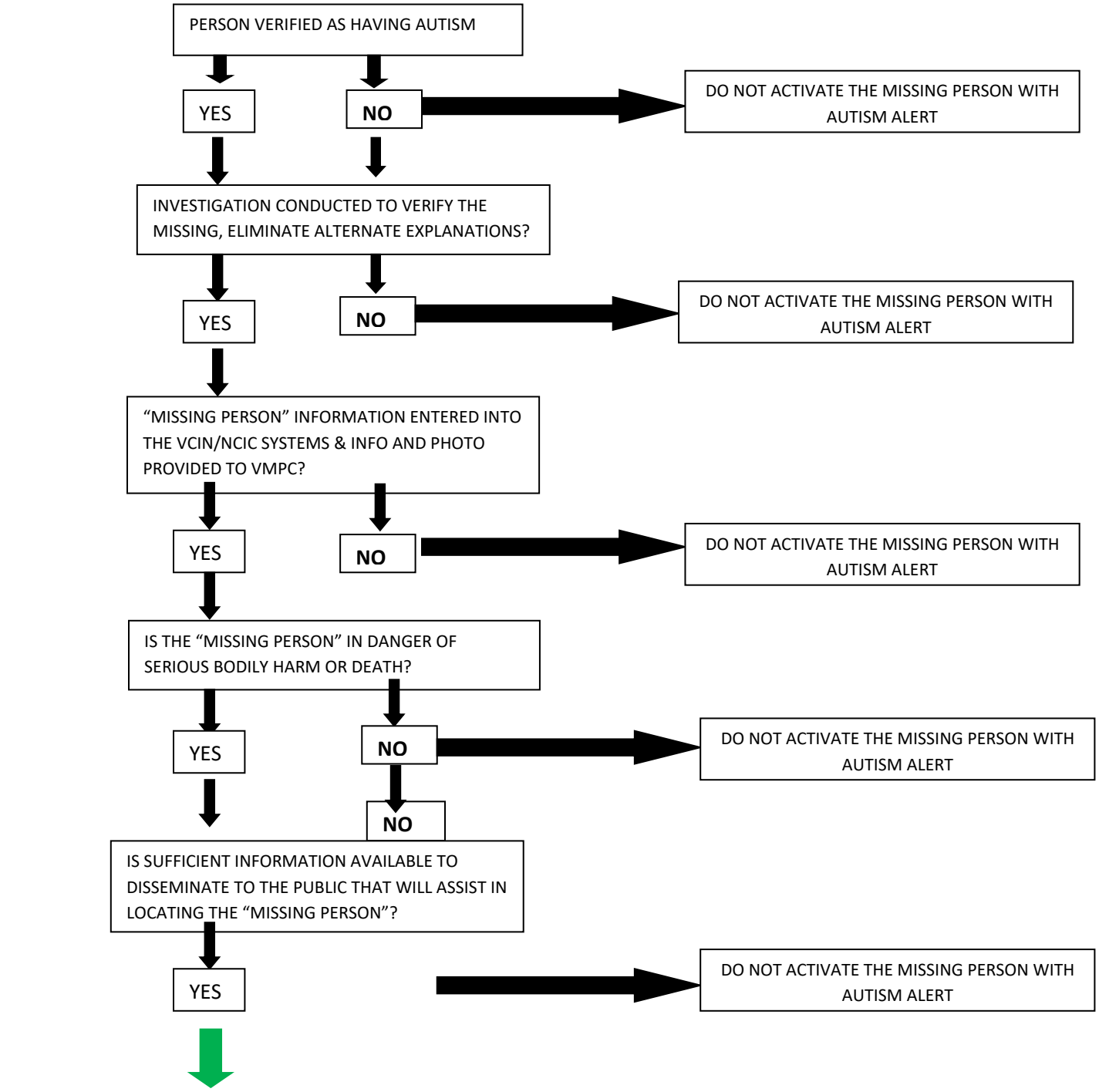
2. Notify VMPC by telephone and immediately confirm our receipt of the packet information. If you should have any difficulties transmitting information, designate a department contact for VMPC (include a name and telephone number on the standardized form).

3. Forward the most current photograph of the missing person immediately and forward all incident details or summaries to the Virginia Missing Person Clearinghouse at vamissing@vsp.virginia.gov and dutysgthq@vsp.virginia.gov. The electronic image of the photograph must be in Joint Photograph Experts Group (JPEG) format.

Telephone #: 804-674-2026 **Forms only – Facsimile #: 804-674-6704**

4. The Virginia State Police will contact any/all broadcasting companies through the Everbridge Alert System upon approval to activate the Virginia "Missing Person with Autism Alert". The Virginia State Police will provide supplemental information through the Everbridge Alert System with a detailed summary of the missing person, and forward a copy of their photograph to any/all broadcasting companies.

DECISION FLOWCHART FOR VIRGINIA "MISSING PERSON WITH AUTISM ALERT" PLAN ACTIVATION



ACTIVATE THE VIRGINIA "MISSING PERSON WITH AUTISM ALERT"

APPENDIX A

VIRGINIA Missing Person with Autism Alert FORMS

Virginia Missing Person with Autism Alert Request Form

Incident Information

Date Missing: _____ (mm/dd/yy) **Time Reported Missing:** _____ (hh:mm)

Location of Incident - last known location:

_____
(Description)

Direction of Travel/Destination:

_____
(City, State, Subdivision)

Vehicle Description:

_____
(Make, Model, Year, Color, License Plate Number and State of Issue)

Missing Person Information

Name: _____
(Last, First, MI)

Gender: _____ (Male/Female) **DOB:** _____ (mm/dd/yy or Approx. Year) **Race:** _____ (Include all Types)

Height: _____ (Feet/Inches) **Weight:** _____ (Lbs.) **Hair:** _____ (Style and Color) **Eyes:** _____ (Color)

Clothing:

Shirt: _____
(Type, Long or Short Sleeve, Color)

Pants: _____
(Type and Color)

Shoes: _____
(Type and Color)

Other: _____
(Type and Color)

Outerwear: _____
(Type and Color)

Additional Significant Identifiers: _____

_____

Medical Needs: _____

OBTAIN A PHOTOGRAPH OF THE PERSON, AND E-MAIL TO THE VIRGINIA MISSING PERSON CLEARINGHOUSE vamissing@vsp.virginia.gov and dutysgthq@vsp.virginia.gov.

Virginia Missing Person with Autism Alert Request Form

CONTACT ORGANIZATION:

Sheriff's Office or Police Department: _____

Contact Person: _____

Telephone Number: _____ **Facsimile Number:** _____

Pager Number: _____ **Cellular Telephone Number:** _____

Date and Time Submitted: _____

Virginia Missing Person with Autism Alert Request Form

AUTHORIZATION FOR RELEASE OF MISSING PERSON INFORMATION

For a period of one year from the execution of this form, the undersigned authorizes full disclosure of all records concerning the missing person to any agent of the state of Virginia, Virginia State Police, or any individual or entity assigned by the Virginia State Police, whether the records are of a public, private, internal, or confidential nature. I direct the release of such information regardless of any agreement I may have made to the contrary with any entity or individual to whom the missing person's information is released or presented. The intent of this authorization is to give my consent for full and complete disclosure of potentially confidential information. Additionally, I understand the duty of the Virginia State Police to release any information to the proper authorities and make other reports as may be mandated by law. I also certify that any person(s) who may furnish such information concerning the missing person shall not be held accountable for giving this information; and I do hereby release such person(s) from any and all liability which may be incurred as a result of furnishing such information. I further release the Virginia State Police, Virginia Broadcasters Association and its agents, and designees under this release, from any and all liability which may be incurred as a result of furnishing such information. A photocopy of this release form will be valid as an original thereof, even though the said photocopy does not contain an original writing of my signature. I have read and fully understand the contents of this "Authorization for Release of Information."

PLEASE PRINT OR TYPE:

_____

Last Name, First Name, Middle Initial

_____

Current Address, House Number/Box Number Street Name/Rural Route, City, State, Zip Code

Signature _____

LIABILITY AGREEMENT:

I hereby agree the information I have provided to you acting as an agent of the state of Virginia, Virginia State Police, Virginia Broadcasters Association or any individual or entity assigned by the Virginia State Police, to be truthful, factual, and correct. As the parent/legal custodian, I am aware that in order for the Virginia State Police to activate the Virginia "Missing Person with Autism Alert," the following criteria must be met:

1. The missing person has been diagnosed with autism spectrum disorder
2. The missing person is ***believed to be in danger of serious bodily harm or death***.

I am also aware I may be charged criminally for committing the crime of knowingly providing false information to law enforcement authorities. I have read and fully understand the contents of this "Liability Agreement."

PLEASE PRINT OR TYPE:

_____

Last Name, First Name, Middle Initial

_____

Current Address, House Number/Box Number Street Name/Rural Route, City, State, Zip Code

Signature: _____

Virginia Missing Person with Autism Alert Termination Form

We are terminating the Missing Person with Autism Alert originated by our agency. Please broadcast the following information as necessary.

Text Follows

The Missing Person with Autism Alert which was transmitted earlier for

(Full name) _____ , missing from

(Street) _____

(City or County) _____ , has been

canceled. The "Autism Alert" for (Full name) _____

has been cancelled.

_____

If there are any problems with or questions about the contents of this fax, call

at

_____ _____

(*NAME*) (*PHONE*)

Text Ends

Originating Agency: _____

334 I Speak Language Flashcards.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Language Identification Flashcard ✓

☐	**Arabic**	أنا أتحدث اللغة العربية
☐	**Armenian**	Ես խոսում եմ հայերեն
☐	**Bengali**	আমী ঝংলা কথা ঝেলতে পারী
☐	**Cambodian**	ខ្ញុំនិយាយភាសាខ្មែរ
☐	**Chamorro**	Motka i kahhon ya yangin ûntûngnu' manaitai pat ûntûngnu' kumentos Chamorro
☐	**Dinka**	Riŋp ëkënë yic të yïjam në thunjäy ye tök, ku kor raan Bï yï geer thok.
☐	**Simplified Chinese**	如果你能读中文或讲中文，请选择此框。
☐	**Traditional Chinese**	如果你能讀中文或講中文，請選擇此框。
☐	**Croatian**	Govorim hrvatski
☐	**Czech**	Mluvím česky
☐	**Dutch**	Ik spreek het Nederlands
☐	**English**	I speak English

Language Identification Flashcard ✓

☐	**Farsi**	من فارسی صحبت می کنم
☐	**French**	Je parle français
☐	**German**	Ich spreche Deutsch
☐	**Greek**	Μιλώ τα ελληνικά
☐	**Haitian Creole**	M pale kreyòl ayisyen
☐	**Hindi**	मैं हिंदी बोलता हूँ ।
☐	**Hmong**	Kuv has lug Moob
☐	**Hungarian**	Beszélek magyarul
☐	**Ilocano**	Agsaonak ti Ilokano
☐	**Italian**	Parlo italiano
☐	**Japanese**	私は日本語を話す
☐	**Korean**	한국어 합니다

Language Identification Flashcard ✓

☐	**Laotian**	ຂ້ອຍປາກພາສາລາວ
☐	**Polish**	Mówię po polsku
☐	**Portuguese**	Eu falo português do Brasil *(for Brazil)*
☐	**Portuguese**	Eu falo português de Portugal *(for Portugal)*
☐	**Romanian**	Vorbesc româneşte
☐	**Russian**	Я говорю по-русски
☐	**Serbian**	Ја говорим српски
☐	**Slovak**	Hovorím po slovensky
☐	**Spanish**	Yo hablo español
☐	**Somali**	Waxaan ku hadlaa af-Soomaali
☐	**Tagalog**	Marunong akong mag-Tagalog
☐	**Thai**	พูดภาษาไทย

Language Identification Flashcard ✓

☐	**Tongan**	Maaka ʻi he puha ni kapau ʻoku ke lau pe lea fakatonga
☐	**Ukrainian**	Я розмовляю українською мовою
☐	**Urdu**	میں اردو بولتا ہوں
☐	**Vietnamese**	Tôi nói tiêng Việt
☐	**Yiddish**	איך רעד יידיש
☐	**American Sign Language**	

334 Language Identification Flash Cards.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

2004 Census Test

United States Census 2010

LANGUAGE IDENTIFICATION FLASHCARD

☐ ضع علامة في هذا المربع إذا كنت تقرأ أو تتحدث العربية.	1. Arabic
☐ Խնդրում ենք նշում կատարեք այս քառակուսում, եթե խոսում կամ կարդում եք հայերեն:	2. Armenian
☐ যদি আপনি বাংলা পড়েন বা বলেন তা হলে এই বাক্সে দাগ দিন।	3. Bengali
☐ ឈូមបញ្ជាក់ក្នុងប្រអប់នេះ បើអ្នកអាន ឬនិយាយភាសា ខ្មែរ។	4. Cambodian
☐ Motka i kahhon ya yangin ûntûngnu' manaitai pat ûntûngnu' kumentos Chamorro.	5. Chamorro
☐ 如果你能读中文或讲中文，请选择此框。	6. Simplified Chinese
☐ 如果你能讀中文或講中文，請選擇此框。	7. Traditional Chinese
☐ Označite ovaj kvadratić ako čitate ili govorite hrvatski jezik.	8.Croatian
☐ Zaškrtněte tuto kolonku, pokud čtete a hovoříte česky.	9. Czech
☐ Kruis dit vakje aan als u Nederlands kunt lezen of spreken.	10. Dutch
☐ Mark this box if you read or speak English.	11. English
☐ اگر خواندن و نوشتن فارسي بلد هستيد، اين مربع را علامت بزنيد.	12. Farsi

DB-3309

U.S. DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. CENSUS BUREAU

☐ Cocher ici si vous lisez ou parlez le français.	13. French
☐ Kreuzen Sie dieses Kästchen an, wenn Sie Deutsch lesen oder sprechen.	14. German
☐ Σημειώστε αυτό το πλαίσιο αν διαβάζετε ή μιλάτε Ελληνικά.	15. Greek
☐ Make kazye sa a si ou li oswa ou pale kreyòl ayisyen.	16. Haitian Creole
☐ अगर आप हिन्दी बोलते या पढ़ सकते हों तो इस बक्स पर चिह्न लगाएँ।	17. Hindi
☐ Kos lub voj no yog koj paub twm thiab hais lus Hmoob.	18. Hmong
☐ Jelölje meg ezt a kockát, ha megérti vagy beszéli a magyar nyelvet.	19. Hungarian
☐ Markaam daytoy nga kahon no makabasa wenno makasaoka iti Ilocano.	20. Ilocano
☐ Marchi questa casella se legge o parla italiano.	21. Italian
☐ 日本語を読んだり、話せる場合はここに印を付けてください。	22. Japanese
☐ 한국어를 읽거나 말할 수 있으면 이 칸에 표시하십시오.	23. Korean
☐ ໃຫ້ໝາຍໃສ່ຊ່ອງນີ້ ຖ້າທ່ານອ່ານຫຼືປາກພາສາລາວ.	24. Laotian
☐ Prosimy o zaznaczenie tego kwadratu, jeżeli posługuje się Pan/Pani językiem polskim.	25. Polish

U.S. DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. CENSUS BUREAU

☐ Assinale este quadrado se você lê ou fala português.	26. Portuguese
☐ Însemnaţi această căsuţă dacă citiţi sau vorbiţi româneşte.	27. Romanian
☐ Пометьте этот квадратик, если вы читаете или говорите по-русски.	28. Russian
☐ Обележите овај квадратић уколико читате или говорите српски језик.	29. Serbian
☐ Označte tento štvorček, ak viete čítať alebo hovoriť po slovensky.	30. Slovak
☐ Marque esta casilla si lee o habla español.	31. Spanish
☐ Markahan itong kuwadrado kung kayo ay marunong magbasa o magsalita ng Tagalog.	32. Tagalog
☐ ให้กาเครื่องหมายลงในช่องถ้าท่านอ่านหรือพูดภาษาไทย.	33. Thai
☐ Maaka 'i he puha ni kapau 'oku ke lau pe lea fakatonga.	34. Tongan
☐ Відмітьте цю клітинку, якщо ви читаєте або говорите українською мовою.	35. Ukranian
☐ اگر آپ اردو پڑھتے یا بولتے ہیں تو اس خانے میں نشان لگائیں۔	36. Urdu
☐ Xin đánh dấu vào ô này nếu quý vị biết đọc và nói được Việt Ngữ.	37. Vietnamese
☐ באצייכנט דעם קעסטל אויב איר לייענט אדער רעדט אידיש.	38. Yiddish

U.S. DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. CENSUS BUREAU

MadiSon County School SRO MOU.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

MEMORANDUM OF UNDERSTANDING (MOU)

MADISON COUNTY, VIRGINIA

This MOU is being executed by the below listed entities on August 2021

Madison County, Virginia School District
Madison County, Virginia Sheriff's Office

I. Purpose

This MOU establishes and delineates the mission of the School Resource Officer Program, herein referred to as the SRO Program, as a joint cooperative effort. Additionally, the MOU clarifies roles and expectations and formalizes relationships between the participating entities to foster an efficient and cohesive program that will build a positive relationship between police officers, school staff, and the students, promote a safe and positive learning environment and decrease the number of youths formally referred to the juvenile justice system.

II. Mission

The mission of the SRO Program is to promote school safety by building a positive school climate in which everyone feels safe, and students are supported to succeed. The SRO Program also seeks to reduce violent crime committed by and against youth in our community. The SRO Program accomplishes this mission by supporting safe, secure, and orderly learning environments for students, teachers, and staff. SROs will establish a trusting channel of communication with students, parents, and teachers and establish regular feedback opportunities. The role of the SRO is not to enforce school discipline or punish students. SROs will serve as positive role models to instill in students' good moral standards, good judgment and discretion, respect for other students, and a sincere concern for the school community. SROs will provide information on community resources available to students and parents. Goals and objectives are designed to develop and enhance rapport between youth, families, police officers, school administrators, and the community to promote overall student achievement and success.

III. Goals of the SRO Program

SRO program goals include:

1. To ensure a safe learning environment for all children and adults who enter the building.
2. To prevent and reduce potential harm related to incidents of school violence.
3. To foster a positive school climate based on respect for all children and adults in the school.
4. To create partnerships with behavioral health and other care providers in the community for student and family referral.

This SRO program is unique to the community, based on input from the school administration, teachers, faculty, students, families and community members. The program is designed to fulfill three overall roles:

1) Law Enforcement
2) Fostering Positive School Climate /Crime Prevention
3) Education

Law Enforcement Role – SROs are responsible for the majority of law enforcement activities occurring at the school during school hours but not general student discipline. A determination of whether an activity raises to the level of a law enforcement activity shall be made in consultation with a school administrator. Parents, students, teachers, and other school personnel should bring complaints about student misbehavior to the school principal and/or designee, rather than the SRO.

While the enforcement is the role of SROs, alternatives to arrest should be used whenever possible, and arrest of students should be a measure of last resort. The SROs discretion to act remains the same as that of any other police officer/sheriff's deputy.

Fostering Positive School Climate /Crime Prevention – One of the primary role's SROs fulfill is fostering a positive school climate through relationship-building and crime prevention. Officers will engage in various activities, in consultation with school administration, teachers, and students, and should strive to build a school culture of open communication and trust between and among students and adults by focusing on officers getting to know students at the school, serving as a role model, and working with teachers and administrators to identify students who may be facing challenges and need additional resources or attention to be successful in school. Crime prevention activities include foot patrols, monitoring previous crime locations, speaking to teachers about reducing the opportunity for crimes to occur, analyzing possible crime patterns, investigating crimes, and patrolling the parking lots. Officers may also complete security surveys analyzing the physical safety of school property and facilities.

Education –SROs should participate in the school community by becoming a member of the educational team where appropriate, and by representing the law enforcement community to build positive relationships with youth, their families, and school staff.

Whether talking to students in the hallway or delivering a presentation in the classroom, SROs are embedded in the education fabric within the school. SROs are expected to be proactive in creating and taking advantage of educational situations, and school administrators are encouraged to leverage this resource.

IV. Organizational Structure

A. Composition

The SRO Program will consist of full time Sheriff's Office Personnel that are certified Law Enforcement Officers for the State of Virginia and meet all requirements as set forth by the Madison County School District and Madison County Sheriff's Office Rules and Regulations.

B. Officer Recruitment & Selection

School officials and the Sheriff's Office shall agree on guidelines for the selection of officers to serve as SROs. The ultimate selection process and appointment of the SRO is completed by the law enforcement agency.

SROs should meet two general criteria:

1) **Experience as a police officer and commitment to student well-being** – SROs must have a minimum of two years' experience as a patrol officer, be at least 21 years of age and have extensive experience with juvenile assignments. Experience working with youth and an interest in student success, juvenile justice, child and adolescent development and psychology, and creating a positive school climate are essential.

2) **Successful performance** – All candidates should have proven performance as reflected by prior performance evaluations. Candidates should be free of significant disciplinary action.

C. Training Requirements

Prior to entering service as an SRO, officers shall complete a minimum of 40 hours of initial training that covers responsibilities and/or limitations of SROs, Virginia school laws, MOUs, child development, conflict resolution, developmentally informed de-escalation and crisis intervention techniques, working with youth in a school setting and integrating SROs into a positive school environment. In addition, it is recommended that SROs receive additional training each year on topics such as trending school-based law enforcement topics, child development, adolescent psychology, trauma, conflict resolution, mental health and addiction, children with disabilities, juvenile and education law and policy, PBIS, and cultural competence.

V. Operational Procedures

Chain of Command for SRO's: The SRO will be ultimately accountable to the Madison County Sheriff's Office chain of command. However, while at the school, the SRO will be additionally accountable to the principal or their designee. The SRO is expected to cooperate with the school officials, including administrators and faculty. The SRO will abide by school policy and respond to the requests of school officials.

The SRO's activity in the school is guided by the following procedures and supervision and evaluation shall be provided by school officials to effectively support SROs efforts and monitor their progress:

A. Duties

The primary functions of the SRO are to help provide a safe and secure learning environment, foster a positive school climate, reduce/ prevent crime, serve as an educational resource, and serve as a liaison between the school and the Sheriff's Office. Specific daily assignments to accomplish this function will vary by school. The SRO and school principal or designee will meet on a regular basis to discuss plans and strategies to address specific issues or needs that may arise. As required by law, SROs should never be assigned to duties within schools in place of or in lieu of a certified teacher.

Basic responsibilities of the SRO will include but will not be limited to:

1) To enforce criminal law and protect the students, staff, and public at large against criminal activity.
2) Foster mutually respectful relationships with students and staff to support a positive school climate.
3) Provide information concerning questions about law enforcement topics to students and staff.
4) Provide classroom instruction on a variety of topics including, but not limited to, safety, public relations, occupational training, leadership, and life skills.
5) Coordinate investigative procedures between police and school administrators.
6) Handle initial police reports of violent crimes committed on campus.
7) Take enforcement action on criminal matters when appropriate and after consultation with school administrators.
8) Attend school special events as needed.
9) Prepare lesson plans as necessary for the instruction provided.
10) Collect data on SRO activities (arrests, citations, etc.)

B. Uniform

SRO's will be in duty uniform assigned by the Sheriff's Office pertaining to assigned duties.

C. Daily Schedule

To be determined by the commanding officer and the school administrators consistent with the MOU.

D. Absence/ Substitution

The school district and Sheriff's Office should develop and agree on a protocol for assigning and using substitute SROs when regular SROs are unavailable. Substitute SROs should, at a minimum, have the same requisite experience as regular SROs and, ideally, should have had some training in child development, trauma, and conflict resolution in the school environment.

E. Special Events

To be determined by the commanding officer and the school administrators consistent with this Agreement.

F. Summer Activity

SROs should accomplish as much of the required training as possible during the summer months when school is not in session. SROs may still be involved in some summer projects with the school district, however, they will spend the majority of this time on Sheriff's Office assignments.

G. Role in Responding to Criminal Activity

One of the roles of SROs, as law enforcement officers, is to engage in traditional criminal investigation and report taking. As a law enforcement officer, SROs have the authority to issue warnings, make arrests and use alternatives to arrest at their discretion. SROs, however, perform their duties mindful of the parties' common goal of supporting student success. The following procedures will help SROs be as effective as possible in this role:

1) School staff will contact SROs to inform them of all violent or other criminal activity that creates a safety risk that occurs on the school campus. SROs and school officials shall discuss and agree in writing on what levels of violent activity would prompt school officials to notify the SROs. This information will be conveyed to all school staff. In turn, SROs will inform school administration of all criminal activity they observe on the school campus.

2) For any offense on school property, the SRO, working cooperatively with the school administration, will endeavor to avoid arrest and criminal involvement for misdemeanor activity. Certain offenses (felonies), such as sex offenses, weapons offenses, and any offenses of violence, will normally require the filing of charges in consultation with school officials, but should be evaluated on a case-by-case basis.

3) The SRO and school officials shall put into place plans, such as de-escalation techniques, conflict resolution and restorative justice practices, to serve as an alternative to arrest.

H. Role in School Policy Violations

SROs are not school disciplinarians and violations of the student code of conduct or school's rules that are not criminal matters should always be handled by school faculty and staff, not SROs. SROs should not directly intervene unless the situation directly affects an imminent threat to the health, safety, and security of the student or another person in the school and will employ de-escalation techniques as appropriate. School discipline is the

responsibility of the appropriate school administrator and clear guidelines on SRO involvement should be developed and distributed to school staff. The SRO, as a staff member, will report school policy violations through the proper channels to be handled by school administration. It is the responsibility of the SRO to become familiar with the Student Handbook or Student Code of Conduct, but it is not the responsibility of the SRO to enforce the rules in these documents.

I. Data Collection

SROs should submit a monthly activity report to the Superintendent of Schools, building principals, and his/her Sheriff. The report should include descriptions of all activities engaged in by the SRO, including incidents or calls for service, names of students and/or staff involved, student searches, arrests, citations and/or summons issued, and other referrals to the juvenile justice system.

J. Sharing of Information

Communication and information sharing is essential to the success of the SRO program.

1. Sharing of information will be governed by the Virginia Revised Code, the Virginia Administrative Code, Virginia's Public Records Law, and relevant Madison County Sheriff's Office and Madison County School District policies.

2. The sharing of arrest related information by the SRO with school administration upon request or at the direction of the SRO will involve the dissemination of arrest reports and calls for service filed with the Madison Sheriff's Office or from other Police agencies coming into contact with students from Madison County School District.

3. Juvenile fingerprints and photos as part of the arrest record will not be shared by the SRO.

4. If the SRO is aware of information on a student that is officially obtained by the Madison Sheriff's Office, which reflects that the student is in violation of school policies (Student Handbook or Athletic Code), the SRO may forward that information to school administration.

5. If a Juvenile is an uncharged suspect in a crime, his/her information will not be released unless authorized by a command person at the Sheriff's Office.

6. Information which the SRO obtains from school personnel which deals with criminal or possible criminal intelligence will be maintained by the SRO as a criminal justice file. This file may be shared with other Division personnel and Criminal Justice Agencies but will not be part of the student's school record.

7. Hearsay information or rumors will alone, not be the basis for any formal action by the Madison Sheriff's Office. It can be used in an intelligence capacity or to validate the need for further investigation.

8. Any information that is obtained by the SRO that pertains to criminal activity occurring outside the school limits shall be relayed to the Sheriff's Office or proper jurisdiction.

9. When any felony occurs or any crime that prompts a Law Enforcement response to the schools or if a school building is evacuated the SRO shall contact his immediate supervisor as soon as possible.

10. The SRO shall have access to any public records maintained by the school to the extent allowed by law. Law enforcement officials may need confidential information in emergency situations based on the seriousness of the

threat to someone's health or safety, time sensitivity, and the direct relationship of the information to the emergency.

The following procedures should be followed to facilitate a free flow of information between school officials and the SRO:

K. Role in Locker, Vehicle, Personal, and Other Searches

SROs may participate in a search of a student's person, possessions, locker, or vehicle only where there is probable cause to believe that the search will turn up evidence that the student has committed or is committing a criminal offense. SROs will not ask a school employee to conduct a search for law enforcement purposes.

Unless there is a serious and immediate threat to student, teacher, or school safety, the Superintendent of Schools in concert with the building principals shall have final authority in the building.

The SRO may perform searches independent of the school administration only during emergency situations and where criminal activity is suspected.

i. Strip searches of students by SROs are prohibited.

ii. Unless there is a serious and immediate threat to a student, a teacher, or public safety, SROs shall not initiate or participate in other physically invasive searches of a student.

Limits on Interrogations and Arrests

1. **Interrogations** –SROs may participate in the questioning of a student about conduct that could result in criminal charges only after informing the student of his or her Miranda rights in age-appropriate language and informing the student's parent(s) or guardian(s). Parents/guardians should be allowed sufficient time to arrive at school to be present for interrogation.

2. **Arrests** –Incidents involving public order offenses, including disorderly conduct, profanity, and fighting that do not involve serious physical injury or a weapon, should be considered school discipline issues to be handled by school officials rather than criminal law issues warranting formal law enforcement intervention.

    i. Building principals and the Superintendent or her designee shall be consulted prior to an arrest of a student when practical.

    ii. The student's parent(s) or guardian(s) shall be notified of his or her arrest immediately or as soon as practical and in a timely manner.

    iii. Unless there is a serious and immediate threat to student, teacher, or public safety, SROs shall not use physical force or restraints on students.

L. Role in Critical Incidents

The SRO will be familiar with the emergency operations manual of the Madison County School District. During critical incidents occurring when the SRO is present, the SRO will normally act as a liaison between school administration, police personnel, and other emergency resources if practical.

M. Role in Truancy Issues

Truancy will be handled by school personnel. The SRO will not take an active role in the tracking of truants. The SRO will act as a liaison between the school and police personnel should police involvement become necessary due to safety concerns.

VI. School District Responsibilities

The Madison County School District shall provide the SRO of each campus and any SRO supervisor the following materials and facilities, which are deemed necessary to the performance of the SRO's duties:

1) Access to a properly lighted private office, which shall contain a telephone, a secure computer and printer, which may be used for general business purposes.
2) A location for files and records which can be properly locked and secured.
3) A desk with drawers, chair, worktable, filing cabinet, and office supplies.
4) The opportunity for SROs to address teachers, school administrators and student families about the SRO program, goals, and objectives.
5) The opportunity to provide input regarding criminal justice problems relating to students.
6) The opportunity to address teachers and school administrators about criminal justice problems relating to students during in-service workdays.
7) The District Emergency Operations Manual, Crisis Plan, Student Handbook/Code of Conduct and other related materials as deemed appropriate.
8) School staff designee for referrals for counseling and other school-based and/or community based supportive services for students and families.
9) SROs shall respect the sensitive nature of student privacy and shall abide by all applicable confidentiality, privacy policies, and applicable laws.
10) Encourage attendance for Assistant Principals/SRO's at NASRO (National School Safety Conference).
11) Provide training to teachers, administrators, staff and SROs about when to directly involve SROs with student misconduct and about available alternatives to arrest.

VII. CRISIS PLANNING

Madison County School District and the Madison Sheriff's Office and Fire/EMS Department will coordinate Crisis Planning and training. Each entity will be involved in updates and creation of new Crisis Plans. Consistency throughout the district should be adhered to.

Lock down drills shall be included as part of the district's preparedness plan. Madison County Sheriff's Office shall be included in the creation of lock down procedures so that first responders are familiar with procedures. Lock down procedures should be trauma-informed and consistent throughout the district.

VIII. Reviewing the MOU and SRO Program

The assigned parties shall review the MOU/SRO Program annually and make adjustments as needed. Any revisions will be reflected in an updated MOU.

Complaints against the SRO shall follow the normal complaint process of the Madison County Sheriff's Office and include notice to the appropriate school administrators. This process will be made known to parents and students by school officials.

IX. PROBLEM RESOLUTION

Unforeseen difficulties or questions will be resolved by negotiation between the Superintendent of Madison County School District and the Madison County Sheriff's Office or their designees.

SIGNATURE OF PARTIES & SIGNATURE DATE

Name, Agency, Title	Date
Name, Agency, Title	Date

317 Virginia Senior Alert Termination Fax Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Virginia "Senior Alert" Termination Form

We are terminating the "Senior Alert" originated by our agency. Please broadcast the following information as necessary.

Text Follows

The "Senior Alert" which was transmitted earlier for

(Full name) _____ , missing from

(Street) _____

(City or County) _____ , has been

canceled. The "Senior Alert" for (Full name) _____

_____ has been cancelled.

If there are any problems with or questions about the contents of this fax, call

_____ at _____

(*NAME*) (*PHONE*)

Text Ends

Originating Agency: _____

311 VA Summary of Crime Victim and Witness Rights Act.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office



A Summary of Virginia's Crime Victim and Witness Rights Act

Your Rights and Responsibilities

Department of Criminal Justice Services

Victims Services Section

December 2008

www.dcjs.virginia.gov



Table of Contents

Introduction 1

Definition of Victim 1

Who Can Help 1

The Right to be Informed 2

Confidentiality 2

Important Reminders 2

Protection 2

Victim Safety and Protective Orders 2

Financial Assistance 3

Restitution 3

Victims' Compensation 3

Property Return 3

Compensation for Witnesses 3

Civil Actions 3

Notice of Court Dates and Other Court-Related Assistance 3

Notice of Court Dates 3

Notice of Defendant or Prisoner Status and VINE 3

Employer Intercession 4

Separate Waiting Areas 4

Right to Remain in Courtroom 4

Interpreters 4

Closed Preliminary Hearing 4

Closed Circuit Television Testimony 4

Victim Input 5

Right to Plea Agreement Consultation 5

Victim Impact Statement 5

Post-Trial Assistance and Other Notices 5

Post-Trial Assistance Available 5

Notice of Release on Bail 5

Notice of Direct Appeals & Habeas Corpus Proceedings 5

Parole and Parole Input 5

"Injustice anywhere is a threat to Justice Everywhere"

–Martin Luther King

Introduction

This brochure provides information about the rights and responsibilities of crime victims and witnesses under the 'Crime Victim and Witness Rights Act' (sometimes called the Victims Bill of Rights) and related laws.

These victims' rights laws focus on the provision of information and assistance to victims as their cases proceed through the criminal justice process. Victim/Witness programs, and other local victim assistance programs, can also provide information, support, and assistance to victims outside the formal criminal justice process.

This brochure and other victim assistance brochures and information are available at www.dcjs.virginia.gov/victimsrights

Generally, victims statutory rights and responsibilities fall within the following areas covered by this brochure: Protection, Financial Assistance, Notice of Court Dates and Other Court-Related Assistance, Victim Input, and Post-Trial Assistance and Other Notices.

Definition of Victim

The Victims Bill of Rights and most other victims' rights laws recognize the following individuals as crime victims in Virginia: *Anyone suffering physical, emotional or financial harm as a direct result of a felony or certain misdemeanors. (The misdemeanors are: assault and battery, assault and battery against a family or household member, stalking, sexual battery, attempted sexual battery, and driving while intoxicated).*

The definition of victim includes:

- Spouses and children of all victims
- Parents and guardians of minor victims
- Parents, guardians, and siblings of mentally or physically incapacitated victims or victims of homicide
- Foster parents or other caregivers, under certain circumstances

The Victims Bill of Rights is intended to ensure that crime victims:

- Have opportunities to make the courts aware of the full impact of crime;
- Are treated with dignity, respect, and sensitivity and that their privacy is protected;
- Are informed of their rights;
- Receive authorized services; and,
- Are heard at all critical stages of the criminal justice process.

Who Can Help

If you have been the victim of a crime, it may help to talk with a knowledgeable and understanding person about your feelings. This is difficult, but most victims report that they feel better after freely and confidentially discussing concerns and emotions they are experiencing.

Reach out to someone with whom you feel comfortable. The most important step in recovery is to talk to someone you trust.

There are programs and services available in your area designed to assist victims, their families, and others in dealing with the victimization, and the complexities of the criminal justice system.

You can find out about these services by contacting the office of the local law enforcement agency, commonwealth's attorney or the victim/witness, sexual assault, domestic violence, or child abuse programs in your area. Telephone numbers for these agencies and programs should be in your local phone book.

For information, assistance, and referrals you can also call statewide toll-free numbers including:

- Virginia Crime Victim Assistance INFO-LINE
  1-888-887-3418
- Virginia Family Violence and Sexual Assault Hotline 1-800-838-8238 (V/TTY)

The Right to be Informed

To help to ensure that crime victims are informed of their rights, the law requires that investigating law enforcement agencies (for example, police departments or sheriffs' offices) provide victims with written information about their rights, including their right to leave from work to attend court. Victims should be given a telephone number to call in order to receive further information and assistance regarding their rights. They should also be provided with the names, addresses, and telephone numbers of the Commonwealth's Attorney and the investigating law enforcement agency.

Your local law enforcement agency may use this brochure as part of its effort to assist you and to meet this requirement.

Confidentiality

Crime victims, and certain witnesses, have the right to request that certain information remain confidential. For example, a crime victim may request that courts, police departments, sheriff's offices, commonwealth's attorneys, defense attorneys, and the Department of Corrections not disclose, except among themselves, his or her home address, telephone number, or place of employment. To request confidentiality, the victim must file a Request for Confidentiality by Crime Victim Form (DC-301) with the magistrate, court, commonwealth's attorney, police department or sheriff's office in the locality where the crime occurred. Forms may be obtained from the magistrate or clerk of court. You can consult with the commonwealth's attorney to get a clear idea of what information may be kept confidential in your case.

With some exceptions, law enforcement agencies may not disclose information which directly or indirectly identifies victims of sexual assault or sexual abuse.

Additionally, victims of sexual assault or sexual abuse may request that any Court of Appeals or Virginia Supreme Court decisions not contain their first and last names.

Important Reminders:

1. Victim/Witness programs, and other victim assistance programs, are available to assist you and to provide information, so that you can make informed decisions.
2. Not all rights and services are applicable in every case.
3. To receive information and assistance, victims also have certain responsibilities, including having to file requests to be notified or offer input. For example, to receive notices regarding release of offenders, court dates, and appeals etc., victims are required to provide contact information to certain agencies. To protect your rights to receive notices and offer input, it is extremely important that you ensure that the commonwealth's attorney and other agencies have accurate contact information. VINE (Victim Information and Notification Everyday) is an automated system which automatically notifies registered victims about changes in custody status of particular offenders. For more information about the VINE Program see www.vinelink.com or call 1-800-467-4943.
4. Victims' responsibilities related to receiving notices and offering input are summarized in this brochure. Your local victim/witness program can provide further information.

Protection

Victim Safety & Protective Orders

Virginia has a number of laws that promote victim safety and offender accountability. These include laws authorizing protective orders. It is important to remember, however, that while protective orders may offer you legal protection, they cannot necessarily protect you from violence.

If you believe that you are in immediate danger, dial 911 for assistance. If the danger is not immediate, you may wish to contact your local domestic violence, sexual assault, or victim/witness program to discuss your concerns and assess your options. As indicated above, numbers for these programs are listed in your local phone book or may be found by contacting either of the hotlines listed in this brochure.

A protective order is a legal order issued by a magistrate or a judge to protect one person from physical abuse or threatening behavior by another. A protective order can be issued in cases of domestic violence, stalking, and crimes resulting in serious bodily injury, to protect the health and safety of an abused person and his/her family or household members.

More information about protective orders and how to obtain them is available from many sources, including: your local victim/witness program, domestic violence shelter, or the Court Service Unit of the local Juvenile and Domestic Relations District Court. Additionally, brochures on this topic are available at www.dcjs.virginia.gov/victimsrights.

Financial Assistance

Restitution

Under certain circumstances, the defendant may be ordered to repay you, at least partially, for your losses. The commonwealth's attorney and/or victim/witness program staff can provide more information about local restitution procedures and referrals to appropriate local personnel. Court ordered restitution is no guarantee of repayment by the defendant. It is extremely important that the court clerk, or other agency responsible for sending you any restitution collected, have accurate contact information for you.

Victims' Compensation

If you are the victim of a crime in Virginia and if you were injured during the crime or you are the surviving spouse, parent, grandparent, sibling, or child of a victim who dies as a result of a crime, then you may be compensated for certain unreimbursed losses such as loss of earnings, medical and counseling expenses, or funeral expenses.

The commonwealth's attorney and/or victim/witness program staff can advise you on how to apply for victims' compensation and, if necessary, assist you with the application. You may contact the Criminal Injuries Compensation Fund directly by calling 1-800-552-4007. This number is toll-free, statewide.

Property Return

To assist in the investigation and prosecution of certain crimes, law enforcement authorities may hold your property as evidence. The law allows them to photograph and return certain evidence to you before the trial. However, law enforcement may hold your property until after the trial and any appeals. The commonwealth's attorney and/or victim/witness program staff may be able to assist you in the return of your property.

Compensation for Witnesses

Witnesses traveling from out of town may be entitled to payment for mileage, tolls, parking, meals, and lodging for each day's attendance in court. Ask the victim/witness program staff, commonwealth's attorney, or clerk of court whether and how you can be reimbursed.

Civil Actions

Crime victims can bring civil lawsuits against perpetrators or other responsible parties in order to hold them accountable for harm suffered. A civil action may provide compensation for damages not covered by restitution or victims' compensation. Victims have the greatest probability of being fully compensated when they file civil actions in addition to, rather than instead of, seeking restitution or victims' compensation. You will need the help of a private attorney to pursue a civil action.

The National Crime Victim Bar Association provides victims referrals to local attorneys specializing in victim-related litigation. The referral service can be reached at 1-800-FYI-CALL (394-2255) between 8:30 a.m.–5:30 p.m. (EST) Monday through Friday.

Notice of Court Dates and Other Court-Related Assistance

Notice of Court Dates

You must give the commonwealth's attorney your current name, address and telephone number, in writing, if you wish to be notified in advance of the scheduled court dates for proceedings including:

- Preliminary hearings
- Plea agreement hearings
- Trials
- Sentencing hearings

Notice of Defendant or Prisoner Status and VINE

The law indicates that in order to receive notices about the release of a defendant or prisoner, or other status changes, or to offer parole input, appropriate officials (sheriff, Department of Corrections, jail superintendent, Parole Board) must have your complete contact information.

VINE (Victim Information and Notification Everyday) is an automated system which automatically notifies registered victims and others about certain changes in the custody status of particular offenders. Victims and other concerned citizens can register at www.vinelink.com or by calling 1-800-467-4943.

Enrollment in VINE does not substitute for official registration with the Virginia Department of Corrections or some local jails. Contact your local victim/witness program, local jail, or VA DOC Victim Services Unit at 1-800-560-4292 for additional information and assistance.

Employer Intercession

If you are subpoenaed to court, or otherwise required in writing by the court to appear, and you give reasonable notice at your workplace, your employer may not fire you, discipline you, or require you to use vacation or sick leave in order to go to court. However, your employer is not required to pay you for your time in court. If necessary, the commonwealth's attorney or victim/witness program staff can notify your employer of the law that protects you. (See §18.2-465.1)

Whether or not you have been specifically required by the court to appear, the law (§40.1-28.7:2) requires every employer to allow an employee who is a victim of crime to leave work to be present at all criminal proceedings related to a crime against the employee. The term "criminal proceedings" means any proceeding at which the victim has the right or opportunity to appear.

The victim is responsible for providing the employer with materials summarizing victims' rights, the law which authorizes leave to attend criminal proceedings, and any written notice of criminal proceedings received by the employee. This brochure may be provided to employers by victims in order to provide a summary of victims' rights.

Employers may limit the amount of leave provided, if it creates an undue hardship to the employer's business.

Additionally, employers are not required to pay victim/employees who leave work to attend criminal proceedings. Employers may not dismiss or discriminate against a victim/employee who leaves work to attend criminal proceedings.

Separate Waiting Areas

Some courthouses have separate waiting areas for victims and witnesses, in order to provide them privacy and protection from intimidation. If you are worried about having to wait in an area near the defendant or the defense witnesses, contact your local victim/witness program, the commonwealth's attorney's office, or the clerk of court or bailiff at the courthouse, to see if a separate waiting area is available to you.

Right to Remain in Courtroom

Victims have the right to remain in the courtroom during all court proceedings (bail or bond hearings, preliminary hearings, trials, sentencing, etc.) that the defendant attends, unless the judge has determined that the presence of the victim would impair the conduct of a fair trial.

Additionally, in any case involving a victim who is under the age of eighteen, the court may permit an adult chosen by the victim to remain in the courtroom as a support person for the victim.

Interpreters

If you cannot speak English or you are hearing impaired, a court-approved interpreter may be appointed to assist you during the criminal justice process, at no cost to you.

Closed Preliminary Hearing

In cases of sexual assault, preliminary hearings may be closed to the public. You may wish to speak to the commonwealth's attorney to find out if your preliminary hearing can be closed. However, trials are open to the public.

Closed Circuit Television Testimony

To reduce the trauma experienced by child victims and witnesses when they must testify, the law permits the use of closed-circuit television in certain criminal proceedings, including preliminary hearings, involving alleged offenses against children and murder of a person of any age.

Victim Input

Right to Plea Agreement Consultation

If you are a victim of a felony and you submit a request in writing, the commonwealth's attorney must consult with you, either verbally or in writing, regarding the contents of a proposed plea agreement and your views concerning plea negotiations. If you submit to the commonwealth's attorney a written request to receive notice of any proceeding in which a plea agreement will be offered to the court, the commonwealth's attorney is required to provide advance notice, if practicable.

It is important to understand that 1) the commonwealth's attorney directs the prosecution and has authority to enter into a plea agreement, whether or not you agree with it, and 2) the court can accept a plea agreement, about which you were not consulted, given good cause.

Victim Impact Statement

After the defendant is found guilty in circuit court, the judge may consider a Victim Impact Statement(s) in determining the offender's sentence. The Victim Impact Statement gives the victim the opportunity to tell the court, in writing, the impact of the crime(s). Victims may also be given the opportunity to testify, at the sentencing hearing, regarding the impact of the crime(s).

Post-trial Assistance and Other Notices

Post-Trial Assistance Available

After the trial is over, you are eligible to be informed of certain information about the outcome of the case (disposition). The commonwealth's attorney can, except in some cases involving juvenile offenders, provide case disposition information. If the defendant was convicted, this information includes the crimes for which the defendant was convicted and the sentence imposed. If known, information about the defendant's appeal rights can also be provided. Additionally, the commonwealth's attorney may be able to assist you, or provide the telephone number of offices to contact, if the defendant fails to pay restitution, as ordered. Your local victim/witness program can provide further information about available post trial assistance and procedures.

Notice of Release on Bail

Defendants are sometimes able to appeal their convictions or sentences and may be released on bail while those appeals are being considered.

The law indicates that when a defendant is released on bail pending the outcome of an appeal, the jail, or other agency that had custody of the defendant, must notify the victim of the defendant's release, as soon as it is "practicable" to do so.

Please talk with jail or sheriff's office staff or victim/witness program staff about local bail release notification procedures which may include VINE registration.

Notice of Direct Appeals and Habeas Corpus Proceedings

You must give the Attorney General's Victim Notification Program your current name, address, and telephone number, in writing, if you wish to be notified of the filing, status, and disposition of:

- A direct appeal to the Court of Appeals of Virginia and/or Supreme Court of Virginia
- A state and/or federal petition for a writ of habeas corpus

For more information, contact the Attorney General's Victim Notification Program at (804) 371-7763 or 1-800-370-0459.

Parole and Parole Input

Parole was abolished in Virginia for any offender who commits a felony crime, on or after January 1, 1995. Such an offender is not eligible for parole and will serve at least 85 percent of his or her prison sentence.

However, most offenders who committed crimes before January 1, 1995, are eligible to be considered for parole. Crime victims, who wish to have input into the parole process, for parole eligible prisoners, may do so by contacting the Virginia Parole Board, Victim Input Program, 6900 Atmore Drive, Richmond, VA 23225, 1-800-560-4292.

For Additional Information and Assistance in Your Case

To receive further information and assistance regarding your rights, please contact your local victim/witness program. The name, address, and telephone numbers of the **victim/witness program** are as follows:

The name, address, and telephone numbers of the **commonwealth's attorney** are as follows:

The name, address, and telephone numbers of the **investigating law enforcement** agency are as follows:

Statewide Toll-Free Numbers

For information, assistance, and referrals you can also call statewide toll-free numbers including:

- Statewide Toll-Free Victim Assistance INFO-LINE
  1-888-887-3418 (Hours of operation: Monday through Friday 9 a.m.–5 p.m.)
- Virginia Family Violence and Sexual Assault Hotline 1-800-838-8238 (V/TTY)

or visit our website at
www.dcjs.virginia.gov/victimsrights

This project is supported in part by Grant #2005-VA-GX-0031 awarded to the Virginia Department of Criminal Justice Services by the U.S. Department of Justice. Points of view or opinions contained in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Use of Force Report.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Madison County Sheriff's Office

Use of Force Report

General Order 300

Case # ____ - _____ Date: _____ Day of Week: _____ Time: _____ hrs.

Street Address: _____ Sector: _____

Location Description: _____

Suspect# ____ Last Name _____ First _____ M.I. _____

Address: _____ Phone #: _____

City State Zip

D.O.B. _____

Soc # _____ Race: _____ Hispanic: ☐ Y ☐ N Sex: _____ Hgt. _____ Wgt. _____

Police Force Used:
(check all that apply)

- ☐ Physical Control
- ☐ TASER – Display
- ☐ TASER – Discharge
- ☐ Less Lethal Impact Munitions
- ☐ Canine - Release
- ☐ Canine - Release & Bite
- ☐ ASP
- ☐ Firearm - Discharge
- ☐ Firearm - Display
- ☐ Ripp-Hobble Restraint
- ☐ Other: _____

Suspect Force Used:
(check all that apply)

- ☐ Blunt object
- ☐ Cutting instrument
- ☐ Firearm
- ☐ Other: _____

Effect of Force: (check one in each column)

Suspect	Police	
	☐	1. No visible injury and no complaint of injury.
☐	☐	2. No visible injury, complaint of minor pain.
☐	☐	3. Minor visible injury (bruising, swelling, redness).
☐	☐	4. Injury, requiring medical treatment.
☐	☐	5. Injury requiring overnight hospitalization.
☐	☐	6. Deceased.
☐	☐	7. Other: _____

☐ Photographs of Injury ☐ TASER Evidence Collected Serial Number of TASER: _____

Serial # of TASER Cartridge(s): _____

Describe Suspect/Police Injury: _____

Medical Treatment Provided by Rescue: ☐ Transported to hospital ☐ Refused Treatment: ☐ Y ☐ N

Name of Hospital: _____ Name of Attending Doctor: _____

List charges: _____

Previous Criminal History: ☐ Yes ☐ No

Was suspect using: ☐ Alcohol ☐ Drugs ☐ Mental Health Crisis

Witness: Last Name: _____ First: _____ D.O.B: _____

Address: _____ Phone H#: _____ W#: _____

City State Zip

Witness: Last Name: _____ First: _____ D.O.B: _____

Address: _____ Phone H#: _____ W#: _____

City State Zip

Describe in detail, the actions of the officer(s) and the actions and conduct of the suspect(s) before, during and after the force.

Reporting Ofc. Signature Unit # Date Supervisor Signature Date

Reviewed by Captain: _____ Date: _____

Reviewed by Sheriff: _____ Date: _____

Reviewed by IA: _____ Date: _____

Follow-up meeting w/Officer By: _____ Date: _____

Citizen Complaint (Rev. March 2022).pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

MADISON COUNTY SHERIFF'S OFFICE
CITIZEN COMMENDATION/COMPLAINT FORM

115 CHURCH STREET, MADSION VA 22727
Tel: 540-948-5161
mcsheriff@madisonco.virginia.gov

☐ **COMMENDATION** ☐ **COMPLAINT**

Instructions: If you wish to bring the conduct of a Madison County Sheriff's Office employee to the attention of the Sheriff, favorable or otherwise, please do so by providing as much of the information requested on this form as possible. If it is determined that your complaint merits further inquiry, a special investigator will be assigned. Depending upon the nature of your comments, you may be contacted to provide further information. The report of the special investigator will be reviewed by the Sheriff of Madison County and final disposition will be made by the Sheriff. If you wish, you may submit this form anonymously. However, if you do so, it will not be possible to obtain further details from you or to inform you of the result of our inquiry.

Today's Date (Month day, year):	*Complaint ID No: (For police use only)*

Your Contact Information (not required)

Last Name:	*First Name:*	*M.I.*	*Date of Birth*	
Street Address and Apt. No.:	*City:*	*State:*	*Zip Code:*	
Telephone Number:	*Email Address:*		*Race:*	*Sex:*

Information about the incident

Nature of Incident:	*Police Case No. (if applicable):*	
Location of Incident:	*Date of Incident:*	*Time of Incident:*
Officer(s) or employee(s) Involved (Name, badge number, description, etc.):	*Is there a recording of the incident? If so, describe):*	

Nature of Action: (Circle all that apply)

Extremely helpful and caring	Excessive force	Discourteous or disrespectful
Courageous	False arrest	Vulgar language
Polite & professional	Unlawful search	Sloppy appearance
Highly motivated	Dishonesty	Unknowledgeable
Responsive	Corruption	Other

I hereby swear and affirm that the information provided by me is true, accurate and complete to the best of my knowledge and belief. I understand that any intentionally false, misleading or untrue statements, accusations or allegations herein made by me, either orally or in writing, to any public official investigating the matters addressed herein may subject me to civil liability and/or criminal prosecution.

Signature (<u>not</u> required):	*Print name (<u>not</u> required):*	*Date (Month day, year):*
Signature of receiving supervisor:	*Print name:*	*Date (Month day, year):*

Narrative
Please print neatly! Describe the situation in as much detail as possible. If necessary, continue on additional pages. Be sure to provide the names and contact information for any witnesses whose identities are known to you. If available, provide photographs and/or audiovisual recordings of any of the events described by you.
☐ ***See additional page(s) attached***

Dispositio			
☐ ***Sustained***	☐ ***Exonerated***	☐ ***Unfounded***	☐ ***Referred for Other Action***

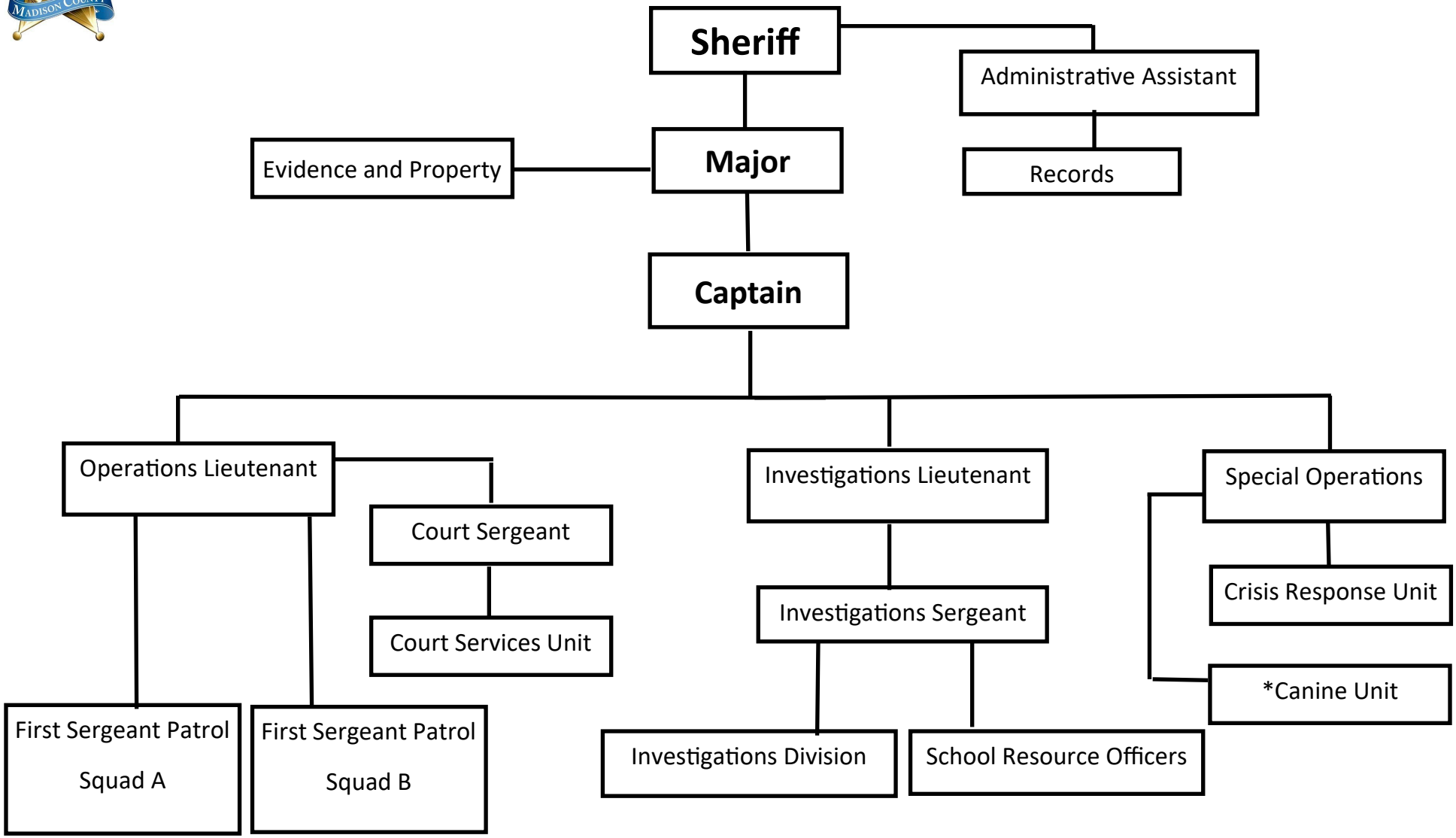
Signature of investigating supervisor:	***Print name:***	***Date (Month day, year):***

Upon completion, route completed form, investigation and recommendations, if any, to the office of the Sheriff. .

200 VA Madison County Sheriffs Department Organizational Chart.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Madison County Sheriff's Office Organizational Structure



Erik J. Weaver, Sheriff

*when applicable

2020 Madison County - Basic Emergency Operations Plan.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Basic Plan

1.0 Purpose – The purpose of the Emergency Operations Plan is to establish the legal and organizational basis for operations in Madison County in response to any type of disaster or large-scale emergency situation. It assigns broad responsibilities to local government agencies and support organizations for disaster mitigation, preparedness, response, and recovery. These responsibilities are generally extensions of normal, day-to-day functions involving the same personnel and material resources. Supporting plans for all hazards and disasters set forth the concepts and procedures whereby the County can effectively apply available resources to ensure casualties and property damage will be minimized and essential services will be restored as soon as possible following such an emergency or disaster situation.

2.0 Situation

2.1 Madison County is located in Central Virginia, approximately 94 miles northwest of Richmond, VA and 87 miles southwest of Washington D.C. at latitude 38^{o} and longitude 78^{o}. It covers approximately 327 square miles and had a population of approximately 13,300 in 2019. Terrain ranges from 800 feet in elevation at Madison Mills, to 4000 feet in elevation in Hawksbill Skyland Drive. The Robinson and Rapidan Rivers are the major waterways in the County.

2.2 The major transportation routes in Madison County are Route 29 (The 29th Division Memorial Highway), a North-South 4-lane highway through the central portion of the County, Route 15 (James Madison Highway) a North-South 2-lane highway on the eastern edge of the County, Route 230, an East-West 2-lane highway on the east side of the County, Route 231, a North-South 2-lane highway through the center of the County. A gas pipeline, operated by Columbia Gas Company, is centrally located in the County west of Route 29.

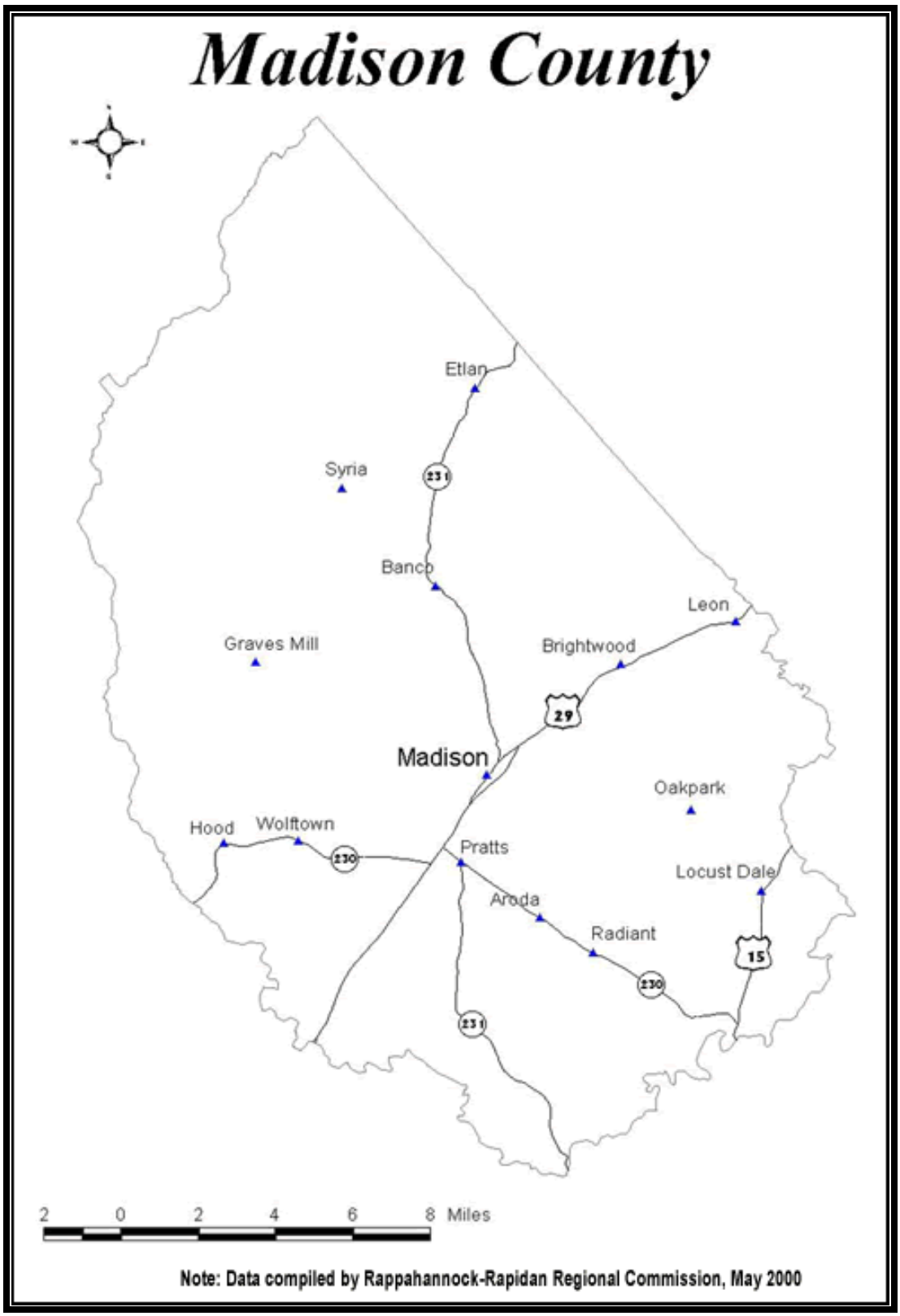
2.3 Based on a hazard analysis of the area, the primary hazards (in priority) in Madison County are floods, hazardous material incidents, severe storms, transportation accidents, fires, dam failures, nuclear power plant accidents, and gas pipeline accidents. For a detailed Hazard Analysis see Tab 2 Support Annex 3: Hazard Mitigation.

2.4 The government of Madison County is responsible for maintaining an emergency plan and response capability to protect the lives and property of its citizens from the effects of both man-made and natural disasters. Additionally, this plan addresses County Government continuity of operations as the Government must continue to function throughout a disaster or emergency situation.

2.5 In accordance with the Virginia Emergency Services and Disaster Law of 2000, as amended, the Madison County Emergency Operations Plan has been developed. This plan will be staffed, revised, exercised, readopted, and reissued once every four years.

THIS PAGE INTENTIONALLY BLANK

Madison County



THIS PAGE INTENTIONALLY BLANK

3.0 Assumptions

3.1 This plan is based on current County response capabilities and assumes they will not change substantially in the next four years.

3.2 County responders are familiar with the plan and have accomplished the training to execute their required tasks.

3.3 Emergencies of various types, size, intensity, and duration will occur within or near the jurisdictional boundaries of the County with or without warning and develop into disasters which affect the safety, health, and welfare of the population and cause damage or destruction to private and public property.

3.4 Notification of an emergency will be accomplished by telephonic or radio communications to the Madison County Emergency Communications Center (911).

3.5 An emergency situation may occur which exceeds local emergency response capabilities. External assistance is available, either through mutual support agreements with nearby jurisdictions and volunteer emergency organizations, or through the Virginia EOC (VEOC). A local emergency must be declared, and local resources must be fully committed before state and federal assistance is requested.

4.0 Organization and Assignment of Responsibilities

4.1 **Emergency Management Organizations** – The Emergency Management organization is a flexible organization and is based on that specified in ESF 5: Emergency Management. It is built on a nucleus composed of the Madison County Sheriff's Office, Madison County Volunteer Fire Company, Madison County EMS, Madison County E-911 and Madison County Emergency Management staff. This basic response organization is augmented, as necessary, by other County agencies and volunteer organizations which are assigned specific tasks in Section VIII. This organization may be expanded further by implementing the Statewide Mutual Aid (SMA) by sending a Request for Assistance to the potential assisting locality and the VEOC (804-674-2400) or by requesting assistance from State and Federal sources. The Chairman of the County Board of Supervisors serves as Director of Emergency Management and is in overall command of any emergency response operation, to include an oil or hazardous material release.

4.2 **Support Agencies** – In the event of an actual or threatened large-scale emergency situation, the above organizations will be augmented by the following departments or agencies which have been assigned emergency duties in addition to their primary day-to-day functions.

4.2.1 Madison County

a. Board of Supervisors
b. Madison County Administrator
c. Madison County School Board
d. Madison County Social Services Department
e. Madison County Health Department
f. Madison County EMS
g. Public Works/Parks and Recreation
h. Building Inspections
i. Department of Planning
j. County Attorney
k. Treasurer/Finance Department
l. County Clerk
m. Commonwealth's Attorney
n. Commissioner of Revenue
o. Madison County Cooperative Extension Office
p. Other County Departments
q. American Red Cross
r. Radio Amateur Civil Emergency Services (RACES)/Amateur Radio Emergency Services (ARES)
s. Civil Air Patrol

4.2.2 State Agencies*

a. Virginia Department of Emergency Management (VDEM) VEOC:
- (800) 468-8892
- (804) 674-2400 (24 hour)

Region II Chief Regional Coordinator
Name: Mark Stone
Mobile: (804) 774-9271
Email: mark.stone@vdem.virginia.gov

Region II Disaster Response and Recovery Officer (DRRO)
Name: Alexa Hussar Boggs
Mobile: (804) 624-1100
Email: alexa.hussar@vdem.virginia.gov

Region II All Hazards Planner
Name: Julio Reyes
Mobile (804) 205-0267
Email: julio.reyes@vdem.virginia.gov

Region II HazMat Officer (HMO)
Name: Craig Strawderman
Mobile: (804) 317-7163
Email: craig.strawderman@vdem.virginia.gov

b. Virginia Department of Environmental Quality:
- Northern Regional Office: (703) 583-3800
- PREP Coordinator: (703) 583-3864

c. Virginia Department of Health: Emergency (after hours): (866) 531-3068
- Madison: (540) 948-5481
- Culpeper: (540) 829-7350
- Fauquier: (540) 347-6400
- Fauquier Environmental Health: 540-347-6363
- Greene: (434) 985-2262

d. Virginia Division of Consolidated Laboratory Services:
- Main DCLS Switchboard: (804) 648-4480
- Emergency After Hours: (804) 335-4617

e. Virginia State Police:
- (800) 572-4510
- Emergencies Only: (800) 552-0962

f. Virginia Department of Transportation
- TOC (540) 332-9500
- Culpeper District: (540) 829-7500
- Engineer/Administrator: (434) 293-0011

g. Virginia Department of Game & Inland Fisheries
- Region 4 Office (Fredericksburg)
  - Main Office: (540) 899-4169
- Region 4 Office (Verona)
  - Main Office: (540) 248-9360

*NOTE: For weekends/holidays/nights (non-business hours) contact VEOC.

4.3 **Emergency Operations Responsibilities** – The Commonwealth of Virginia Emergency Services and Disaster Law of 2000, as amended, provides that emergency services organizations and operations be structured around existing constitutional government. Following is a list of duties and assigned responsibilities for emergency operations in Madison County.

4.3.1 Director of Emergency Management

a. Provide leadership of public organizations for the development and maintenance of this plan, including mutual support agreements with adjacent jurisdictions.
b. Provide overall policy, direction, and control of emergency operations.
c. Represent County in external relationships.
d. Initiate actions to declare a local emergency, when necessary.
e. Continuity of government.

4.3.2 County Administrator

a. Provide advice and assistance to Director of Emergency Management concerning policy, direction, and control of emergency operations.
b. Act as the County Public Information Officer (PIO), and coordinate the release of public information and implementation of rumor control procedures.
c. Provide advice and assistance to the Emergency Management Coordinator concerning direction and control of emergency operations.
d. Recommend declaration of a local emergency when necessary.
e. Assist in identifying essential facilities for continuity of government operations.
f. Assist in disaster assistance and recovery.

4.3.3 Emergency Management Coordinator (EMC)

a. Supervise and coordinate public and private organizations for the development and maintenance of this plan, including mutual support agreements with adjacent jurisdictions.
b. Organize Local Emergency Planning Committee (LEPC).
c. Provide advice and assistance to the incident commander concerning the direction and control of incident site emergency operations.
d. Recommend declaration of a local emergency when necessary.
e. Serve as the Local On-Scene Coordinator (LOSC), when appropriate.
f. Provide direction and coordination for the emergency staff in the EOC when activated.
g. Identify essential facilities for continuity of government operations.
h. Ensure required reports are submitted to the VEOC and other state agencies. Direct notification of Virginia Department of Health if radioactive materials or infectious (etiological) agents are involved and notification of Joint Nuclear Accident Coordinating Center (JNACC) if nuclear weapons are involved.
i. Ensure an accurate record of incident-related expenses is maintained.
j. During Hazardous Materials incidents maintain records of County expenditures and coordinate billing of responsible party.
k. Employ clean-up contractors when necessary.

l. Coordinate with State or Federal authorities in supervision of clean-up activities to ensure proper disposal of contaminated materials.
m. Damage assessment.
n. Coordinate disaster assistance and recovery.
o. Coordinate planning, training, and conducting exercises of this plan.
p. Activate EOC, assign message clerk duties, manage logistics

4.3.4 Deputy Emergency Management Coordinator (DEMC)

a. Will act as EMC in his/her absence
b. Assist in supervising and coordinating public and private organizations for the development and maintenance of this plan, including mutual support agreements with adjacent jurisdictions.
c. Provide advice and assistance to the Incident Commander concerning the direction and control of incident site emergency operations.
d. Recommend declaration of a local emergency when necessary.
e. Activate EOC, assign message clerk duties, and manage logistics.

4.3.5 Madison County Sheriff's Office

a. Enforce all applicable local, State, and Federal laws.
b. Provide assistance to the on-scene commander to:
(1) Warn and evacuate the public as required.
(2) Control access to the area and provide traffic control.
(3) Establish security at the incident scene, as coordinated with the Inc/Com
c. Investigate deaths in coordination with the medical examiner and assist with search and rescue operations.
d. Provide security for evacuated area, vital facilities, and supplies.
e. Assist with investigation and enforcement of illegal or improper hazardous waste management and/or disposal.
f. In coordination with EMC, train Sheriff's personnel in hazardous materials emergency response procedures. (HMERP)
g. Provide representation in the County EOC.
h. Maintain EOC facility and provide logistical support during EOC activation.
i. Assist with reports and records.

4.3.6 Director of E911 Center

a. Maintain a point of contact (ECC/911) for notification and verification of an emergency incident.
b. Provide emergency communications system.
c. Coordinate reverse-911 system for citizen notification
d. Recommend operating channels and frequencies to be used
e. Provide radio units to incoming mutual aide personnel

f. Dispatcher

(1) Maintain a general knowledge of the requirements to submit reports to the VEOC.
(2) Be prepared to act on reports received from facility emergency coordinators, law enforcement officers, private citizens, 911 or telephone operator calls, or any other source.
(3) Obtain as much of the information required on the Hazardous Materials Report as possible.
(4) Dispatch initial response units, providing them as much information as possible.
(5) Alert key officials, to include Sheriff, EMC, DEMC, County Fire Chief, Director Emergency Medical Services and County Rescue Captain. Alert Director of Emergency Management (BOS Chairman) when directed.
(6) Alert neighboring jurisdictions if they may be affected.
(7) Transmit initial and follow-up reports to the VEOC, as directed.
(8) Maintain a formal record of all actions, directions, and communications accomplished or transmitted during an emergency response or disaster operation.

4.3.7 Madison County Volunteer Fire Company

a. County Fire Chief

(1) Coordinate the training and equipping of jurisdiction emergency response units and personnel.
(2) Review and retain facility response plans submitted by oil or hazardous materials facilities.
(3) Maintain a list, by facility, of hazardous materials in designated response sectors and their related Material Safety Data Sheets.
(4) Perform duties in the County EOC, when activated.
(5) When available, serve as Incident Commander for Hazardous Materials incidents.

b. Madison County Volunteer Fire Company

(1) Ensure Fire Department personnel are properly trained and equipped to respond to fire and hazardous materials incidents.
(2) Fire prevention and suppression.
(3) Provide a qualified initial Incident Commander in the event of a fire or Hazardous Materials emergency.
(4) Annually coordinate emergency response plans with specific facilities in response sector, including County and Private Schools.
(5) Maintain a list, by facility, of hazardous materials in the Department's sector and their related Material Safety Data Sheets.

(6) Maintain and exercise response action checklists for each oil or hazardous materials facility to ensure coordination with their emergency response plan.
(7) Develop and exercise SOPs for response to a transportation incident with potential involvement of oil or hazardous materials.
(8) Maintain EOC facility and provide logistical support during EOC activation.
(9) Assist with missing person search and rescue.
(10) Assist with radiological monitoring and decontamination.
(11) Assist with warning and evacuation.
(12) Provide representation in the County EOC, when directed.
(13) Assist with reports and records.
(14) Provide emergency apparatus, equipment and emergency personnel to respond to incidents

4.3.7 Madison County Emergency Medical Services

a. County EMS Chief

(1) Ensure EMS Department personnel are properly trained and equipped to respond to EMS incidents.
(2) Perform duties in the County EOC, when activated.

b. Madison County Emergency Medical Services and Volunteer Personnel

(1) Provide emergency medical transportation and first aid.
(2) If sufficient, qualified personnel are available, provide medical stations in public shelters when an evacuation has been implemented and public shelters are occupied.
(3) Ensure personnel are properly trained and equipped to respond to incidents involving known oil and hazardous materials in the area. (see Hazard Specific Annex 2: Hazardous Material Emergency Response Plan).
(4) Coordinate with Madison County Volunteer Fire Company for access to a list, by facility, in assigned response sector, of hazardous materials and their related Material Safety Data Sheets.
(5) Maintain and exercise SOPs for response to a transportation accident with potential involvement of oil or hazardous materials.
(6) Maintain EOC facility and provide logistical support during EOC activation.
(7) Provide representation in the County EOC, if required.
(8) Assist with reports and records.

4.3.9 Madison County School Board-Superintendent of Schools

a. Develop expedient evacuation procedures for schools.

b. In coordination with the Department of Social Services, the Department of Health, and the Culpeper American Red Cross Chapter, develops plans to provide food and shelter to evacuees in County schools outside the risk area.
c. Provide mass evacuation transportation for evacuation of group facilities or the public, as needed.
d. Provide a representative in the County EOC, if required.
e. Assist with reports and records.

4.3.10 Madison County Department of Social Services

a. Overall coordination of County Shelter Program.
b. Coordinate reception and care of evacuees at shelter centers

(1) Provide registration and record keeping.
(2) Provide mass feeding.
(3) Provide crisis counseling services as required.

c. Provide emergency welfare services for displaced persons.
d. Coordinate the services of quasi-public and volunteer relief organizations such as the American Red Cross and Salvation Army.
e. Management of donations.
f. Provide a representative in the County EOC.
g. Assist with reports and records

4.3.11 Madison County Health Department

a. Assist with hazardous waste management and enforcement.
b. Epidemic control measures, including insect and rodent control, inspection of food, milk, and water supply, and ensuring the continued supply of potable water.
c. Coordinate with the Department of Social Services to provide proper sanitation and health care in shelters.
d. Develop and coordinate operation of mass vaccination/medication clinics, if necessary.
e. Assure the provision of minimum essential sanitation services.
f. Maintain a list of, and issue warnings to, operators of water treatment plants whose water supply may become contaminated as a result of an oil or hazardous materials release within Madison County.
g. Issue health notices to primary care physicians and facilities (ESF 15: External Affairs).
h. Emergency mortuary and interment coordination.
i. Identification of the dead assisted by the Sheriff's Office and State Police.
j. Coordination and control of biologicals and radiologicals.
k. Coordination with regional hospitals to develop plans for use of area hospitals to treat and decontaminate hazardous materials incident victims in response to a mass exposure.

l. Coordinate with University of Virginia Medical Center, Culpeper Regional Hospital, and Martha Jefferson Hospital to provide:

(1) Emergency medical services.
(2) Assistance in expanding medical and mortuary services to temporary facilities within Madison County, other facilities, if needed.
(3) Assistance with reports and records.

m. Provide a representative in the County EOC.
n. Assist with reports and records.

4.3.12 Madison County Facilities and Maintenance Department

a. Assist with emergency response operations as required.
b. Provide heavy equipment, such as front-end loaders and dump trucks, etc., with trained operators.
c. Ensure employees are trained in protective measures.
d. Develop and maintain in-house SOPs for preventing oil or hazardous materials runoff from entering the sewer/storm drain system.
e. Assist in identifying essential government facilities.
f. Assist in response to damage to County's utility systems.
g. Coordinate the maintenance and continued operation of the County's water and sewer systems.
h. Assure the continued supply of potable water.
i. Coordinate the maintenance and continued operation of County facilities.
j. Assist with resource and supply.
k. Assist in traffic control by providing traffic barricades.
l. Assist with decontamination and cleanup, if required.
m. Provide a representative in the County EOC.
n. Assist with reports and records
o. Post the daily notices at the local Post Offices

4.3.13 Madison County Department of Building Inspections and Department of Planning

a. Ensure all construction that occurs within the County is in compliance with the County's comprehensive plan, zoning, and land-use regulations.
b. Conduct inspections to enforce and carry out the jurisdiction's building codes (i.e., structural, mechanical, electrical, etc.).
c. Overall responsibility for coordinating damage assessment in Madison County.
d. Provide two teams of two trained individuals to accomplish damage assessment following a disaster.
e. Inspect buildings following a disaster for structural, electrical, gas, plumbing, and mechanical damage before permitting re-occupancy.
f. Ensure all repairs and rebuilding complies with County's building codes, zoning, and land-use regulations.
g. Develop Resource Inventory.

h. Provide maps, charts, and population data as necessary.
i. Provide a representative in the County EOC, if required.
j. Assist with reports and records.

4.3.14 Madison County Cooperative Extension Office

a. Assist with emergency operations as required.
b. Develop and maintain SOP's for all aspects of the agricultural community and develop plans and response guidelines for dealing with agricultural emergencies and agro security.
c. Take the lead role in response to the County's agricultural community for damage assessment
d. Assist during County emergencies dealing with livestock, livestock welfare, food and water for livestock and the disposal of expired or infected livestock
e. Provide a representative in the County EOC, if required

4.3.15 County Attorney

f. Advise the County concerning legal responsibilities, powers, and liabilities regarding emergency operations and post-disaster assistance.
g. Assist the Board of Supervisors and the County Administrator/Coordinator of Emergency Management with maintaining continuity of government.
h. Implement legal actions as directed to recover expenses from liable parties.
i. Support enforcement of illegal hazardous waste disposal ordinances and regulations.
j. Provide a representative in the County EOC, if required.
k. Assist with reports and records.

4.3.16 Madison County Finance Department

a. Maintain records of all actions taken during emergency operations
b. Maintain records of all expenses during all phases of emergency operations.
c. During Hazardous Materials incidents assist in maintaining records of County expenditures and billing responsible party.
d. Coordinate with department heads to expedite the process of procuring necessary goods and services to support emergency operations.
e. Coordinating with department heads and the real estate assessor during the damage assessment and recovery phases of disaster operations.
f. Coordinate efforts to apply for disaster aid from State and Federal Governments.
g. Provide representative in the County EOC, if required.
h. Assist with reports and records.

4.3.17 County Clerk

a. Assemble and archive records pertaining to emergency operations.
b. Plan for, and transfer, County records if in jeopardy of damage or destruction.

4.3.18 Madison County Commissioner of Revenue/Virginia Cooperative Extension

a. Assist in assessing the overall damage to public and private property.
b. Provide a representative in the County EOC, if required.
c. Assist with reports and records.

4.3.19 Virginia Department of Transportation Madison Residency Office

a. Upon approval from VDOT Headquarters, assist with emergency response operations as requested by County.
b. Coordinate with Public Works to provide heavy equipment, such as front-end loaders and dump trucks, etc., with trained operators.
c. Ensure employees are trained in protective measures.
d. Coordinate with Sheriff's Office to assist in traffic control by providing traffic barricades.
e. Provide a representative in the County EOC.
f. Assist with reports and records.

4.3.20 Radio Amateur Civil Emergency Services (RACES)/Amateur Radio Emergency Services (ARES)

a. Upon request from EMC, or designated representative, coordinate volunteers to assist with emergency response operations to include:

(1) Establish communication stations in EOC and other operations stations in the County, as directed by EMC.
(2) Maintain records of all actions taken and expenses incurred and submit to EMC.
(3) Coordinate with EMC training of volunteers and participation in County training and exercises.

4.3.21 Orange County, Culpeper County, Page County, Rappahannock County, Greene County – Provide assistance, if available and upon request, through mutual aid agreements to:

a. Issue warnings and direct appropriate protective actions for citizens located in threatened areas within their jurisdiction.
b. Be prepared to provide alternate and/or additional evacuation assembly centers and shelters upon request.
c. Assist with coordination of medical facilities.
d. Provide back-up emergency equipment and personnel in accordance with mutual aid agreements upon request.

4.3.22 State Agencies – The Virginia Emergency Operations Center (VEOC) is the common point of contact for Department of Environmental Quality and the Virginia Emergency Response Team. The VEOC is the primary agency for coordinating

response of other state agencies to support local emergency operations. The State Regional Hazardous Materials Officer will provide technical assistance and will be the State On-Scene Coordinator (SOSC) for incidents involving hazardous materials when other state agencies are involved in the response. The Department of Environmental Quality will provide the SOSC for incidents involving oil or hazardous materials which will affect the water resources of the Commonwealth. The Responsible Party has the direct responsibility to ensure that all required/mandatory notifications are accomplished, to include Federal agencies. The State Emergency Operations Center, upon receipt of notification from the Responsible Party and/or County will report oil or hazardous material events, which meet predetermined criteria, to those state agencies which require notification of the event even though direct assistance is not required.

4.3.23 **Federal Agencies** – will provide technical assistance in accordance with their area of responsibility. Other assistance may be provided by agencies within their statutory, regulatory, or discretionary authority.

5.0 Concept of Operations

5.1 General

5.1.1 The Madison County organization for emergency operations consists of existing government departments and private emergency response organizations.

5.1.2 The Chairman of the Board of Supervisors is the **Director of Emergency Management**, who is, with the consent of the balance of the County Board of Supervisors, the constituted legal authority for approving Emergency Operations Plans and declaring a local state of emergency. The day-to-day activities of the emergency preparedness program have been delegated to the EMC and DEMC. The EMC will direct and control emergency operations in time of emergency and issue directives to other services and organizations concerning disaster preparedness.

5.1.3 **Succession to the Director of Emergency Management** will be the Vice Chairman, then other members of the Board of Supervisors in order of seniority.

5.1.4 The Madison County Local Emergency Planning Committee (LEPC), composed of members appointed by the Board of Supervisors, is responsible for the development and maintenance of this plan. Membership in the LEPC, as required by SARA Title III regulations, is composed of the Director of Emergency Management (DEM), representatives from the Madison County Sheriff's Office, Madison County Volunteer Fire Department, Madison County EMS, Madison County E-911, other Madison County departments, news media representatives, interested community groups, facility owners and operators, and staffed primarily by the Madison County Emergency Management Coordinator (EMC). Other interested individuals may petition the LEPC for membership. Meetings will be held annually, or as needed. Each department or agency tasked with a response

role will review the plan annually and provide input for the maintenance of this plan. All plan holders are considered extended members of the committee and will be requested to participate as needed (see Attachment 4).

5.1.5 The LEPC will coordinate the compatibility of the plans and procedures of key facilities and private organizations within the County with the County's Emergency Operations Plan, as appropriate.

5.1.6 The day-to-day activities of the emergency management program, for which the EMC is responsible, include developing and maintaining an EOP, maintaining the County EOC in a constant state of readiness, and other staff actions as requested by the LEPC. The EMC/DEMC will ensure the primary EOC (Sheriff's office conference room) is in a state of constant readiness.

5.1.7 A **local emergency** may be declared by the local director of emergency management with the consent of the governing body of the political subdivision. In the event the governing body cannot convene due to the disaster or other exigent circumstances, the director or in his absence, the deputy director, any member of the governing body may declare the existence of a local emergency, subject to confirmation by the governing body at its next regularly scheduled meeting or at a special meeting within forty-five days of the declaration whichever occurs first (see Section 44-146.21, Virginia Emergency Services and Disaster Law). The declaration of a local emergency activates the Emergency Operations Plan and authorizes the provision of aid and assistance thereunder. It should be declared when a coordinated response among several local agencies/organizations must be directed or when it becomes necessary to incur substantial financial obligations in order to protect the health and safety of persons and property or to provide assistance to the victims of a disaster.

5.1.8 The EMC will notify the Virginia Department of Emergency Management immediately upon the declaration of a local emergency. Daily situation reports will be completed at the end of each day for the duration of local EOC operations and a copy submitted to the State EOC (see ESF 5: Emergency Management). All appropriate locally available forces and resources will be fully committed before requesting assistance from the state. All disaster-related expenditures must be documented in order to be eligible for post-disaster reimbursement should a federal disaster be declared.

5.1.9 **Incident Command System - National Incident Management System (NIMS)**
The initial arriving County emergency response units shall establish on-scene tactical direction and control in accordance with the principles of the Incident Command System (ICS) and the National Incident Management System (see Tab 14 to ESF 5: Emergency Management). If the initial arriving unit is a Virginia State Police unit, that unit will assume initial incident command until appropriate County units arrive on scene. The management of the emergency will transition to

a "unified command", with tactical response units under the supervision of their designated command officer, when the "Responsible Party" representatives, State, Federal, and other external elements arrive on scene. In a hazardous materials incident, the **County Hazardous Materials Officer/EMC, and the Fire Chief or senior rescue official on scene will coordinate the overall utilization of responding County and external units.** Consultant support shall be provided from various agencies with appropriate expertise including environmental, health, transportation, and other sources. **The County Emergency Management Coordinator / Hazardous Materials Officer will provide advice, assistance, and coordinate requests for outside, State, and Federal assistance.** The EMC will also determine if the situation warrants activation of the County Emergency Operations Center (EOC).

The EMC or, in his absence, the DEMC, will determine the need to evacuate large areas and will issue orders for evacuation or other protective action as needed. The Sheriff's Office will implement evacuation and coordinate security for the evacuated area (see ESF 1: Transportation and Evacuation).

5.1.10 The EMC or, in his absence, the DEMC, with support from designated local officials, will exercise direction and control from the EOC during disaster operations. The EOC may be partially or fully staffed depending on type and scope of the disaster. The EOC will coordinate the provision of logistical and administrative support to response personnel deployed to the disaster site(s). Available warning time will be used to implement increased readiness measures which will ensure maximum protection of the population, property, and supplies from the effects of threatened disasters. Citizens will be notified by radio and television announcements, reverse 911, and announcements and directions will be posted at every local Post Office.

5.1.11 The Department of Social Services is responsible for establishing procedures to provide guidance to disaster victims in obtaining post-disaster assistance, such as temporary housing and low-interest loans.

5.1.12 The Madison County Extension Agent along with the Madison County Extension office will be responsible for Agrosecurity preparedness in Madison County. The Madison County Extension agents will be vital in assistance for an agriculture related emergency and will advise the EOC staff with recommendations. The head Extension Agent for the County, will be on the EOC staff. The Extension staff will assist with any agriculture damage assessments and make reports to the EOC staff and make reports for VDEM.

5.1.13 The heads of County Departments will develop and maintain detailed plans and standard operating procedures necessary for their departments to effectively accomplish their assigned tasks and should refer to the appropriate annexes and appendices of this plan. Additional guidance is contained in the County Hazardous Materials Emergency Response Plan. Accurate records of disaster-related expenditures will be maintained. All disaster-related expenditures will be

documented to provide a basis for reimbursement. In time of emergency, the heads of County offices, departments, and agencies will continue to be responsible for the protection and preservation of records essential for the continuity of government operations. Department and agency heads will establish lists of succession of key emergency personnel (see Attachments 1 and 2).

5.1.14 Day-to-day functions that do not contribute directly to the emergency operation may be suspended for the duration of any emergency. Efforts that would normally be required of those functions will be redirected to accomplish the emergency task by the department concerned.

5.1.15 The County must be prepared to bear the initial impact of a disaster on its own. Help may not be immediately available from the State or Federal government after a natural or man-made disaster. All appropriate locally available forces and resources will be fully committed before requesting assistance from the state. The County Administrator's Office will identify sources from which emergency supplies, equipment, and transportation may be obtained promptly when required (see ESF 7: Logistics Management and Resource Support). Requests for assistance will be made through the County EOC and State EOC to the State Coordinator.

5.1.16 Emergency assistance may be made available from neighboring jurisdictions (Orange County, Culpeper County, Page County, Rappahannock County, and Greene County) or emergency forces may be sent from Madison County to assist adjoining jurisdictions. Such assistance will be in accordance with existing mutual aid agreements, with Orange County, Culpeper County, Page County, Rappahannock County and Greene County, including the Statewide Mutual Aid agreement, or, in the absence of official agreements, directed by the EMC, when he determines such assistance is necessary and feasible. If the incident requires the assistance of Federal and/or State agencies, the County fire chief will be designated the Local On-Scene Coordinator (LOSC) to work with the Federal On-Scene Coordinator (FOSC) and the SOSC at the scene of the incident. The Director of Emergency Management, or his designee, will be the Local Coordinating Officer (LCO) to work with the Federal Coordinating Officer (FCO) and the State Coordinating Officer (SCO) to facilitate federal, state, and local coordination remote from the incident site.

5.1.17 Support by Virginia National Guard military units may be requested through the State EOC. Military forces, when made available, will support and assist local forces and may receive from the local Emergency Management Coordinator or his designated representative, mission-type requests, to include objectives, priorities, and other information necessary to accomplish missions.

5.1.18 <u>Declaration of a Local Emergency</u>

a. The County Board of Supervisors, by resolution (see Attachment 3), will declare an emergency to exist whenever the threat or actual occurrence of a

disaster is, or threatens to be, of sufficient severity and magnitude to require significant expenditures and a coordinated response in order to prevent or alleviate damage, loss, hardship, or suffering.

b. A declaration of a local emergency activates the response and recovery programs of all applicable local and interjurisdictional Emergency Operations Plans and authorizes the furnishing of aid and assistance in accordance with those plans. In the event the Board cannot convene due to the disaster, the Director of Emergency Management, EMC, or any other member of the Board of Supervisors in his absence, may declare a local emergency to exist subject to confirmation of the entire Board, within forty-five days. The EMC will advise the State EOC immediately following the declaration of a local emergency.

c. When local resources are insufficient to cope with the effects of a disaster and the County requests state assistance, the following procedures will apply. The Director of Emergency Management, by letter to the State Coordinator of Emergency Management, will indicate a local emergency has been declared, the local Emergency Operations Plan has been implemented, available resources have been committed, State assistance is being requested and, if appropriate, recommends the Governor declare a state of emergency. A copy of the resolution declaring a local emergency to exist should accompany this letter (see Attachment 3). If State assistance is urgently required; a phone call request to the State EOC is sufficient, with the above requirements accomplished later.

5.1.19 The Virginia Emergency Operations Plan requires the submission of the following reports by local government in time of emergency: Situation Report, Damage Assessment Report, and an After-Action Report (reference ESF 5: Emergency Management ; ESF 14: Long-Term Community Recovery ; and ESF 15: External Affairs).

5.1.20 This plan is effective as a basis for training and pre-disaster preparedness upon receipt. It is effective for execution when:

a. Any disaster threatens or occurs in the County and a local disaster is declared under the provisions of Section 44-146.21, the Commonwealth of Virginia Emergency Services and Disaster Law of 2000, as amended.

b. The Governor declares a state of emergency.

5.1.21 The Emergency Management Coordinator (EMC) is responsible for developing and maintaining this plan. Staff support is provided by the EMC. The EOP will be exercised, revised, and **readopted every four years**. It will be updated annually as appropriate. The Virginia Department of Emergency Management will provide guidance and assistance.

This Plan will be distributed only as indicated (see Attachment 4) and will not be reproduced without the specific approval of the Emergency Management Coordinator or designated representative.

5.1.22 Operational Periods (Preparedness, Response, Recovery, Mitigation)

a. **Normal Operations** – Emergency operations plans and procedures will be developed and maintained. Training and test exercises will be conducted periodically as required to maintain readiness.

b. **Increased Readiness** – When a peacetime disaster threatens, all agencies having responsibilities will take action as called for in their respective functional annex. (Example: flash flood watch.)

c. **Emergency Operations** – Full-scale operations and a total commitment of manpower and resources are required to mobilize and respond in time of emergency. The local EOC must direct and control all emergency operations. A local emergency should be declared. Damage assessment begins. There are two phases of emergency operations:

(1) **Mobilization Phase** – Conditions worsen requiring full-scale mitigation and preparedness activities. (Example: flash flood warning.)
(2) **Response Phase** – Disaster strikes. An emergency response is required to protect lives and property.

d. **Recovery** – Recovery is both a short-term and a long-term process. Short-term operations restore vital services to the community and provide for basic needs to the public. Long-term recovery focuses on restoring the community to its normal, or to an improved, state of affairs. Examples of recovery actions are the provision of temporary housing and food, the restoration of non-vital government services, and the reconstruction of damaged areas.

6.0 Training and Exercises

6.1 **Objectives** – Trained and knowledgeable personnel are essential for the prompt and proper execution of the Madison County Emergency Operations Plan and subplans. Madison County will ensure all response personnel have a thorough understanding of their assigned responsibilities in a disaster situation, as well as how their role and responsibilities interface with the other response components of the Madison County Emergency Operations Plan. All personnel will be provided with the necessary training to execute those responsibilities in an effective and responsible manner.

6.2 **Program Design** – The Emergency Management Director, Coordinator, and Deputy Coordinator are responsible for the development, administration, and maintenance of a comprehensive training and exercise program tailored to the needs of Madison County. This program will be comprised of a general core, functionally specific, as well as on-going refresher training programs designed to attain and sustain an acceptable level of emergency preparedness for Madison County.

6.3 **Procedures** – Training will be based on Federal and State guidance. Instructors will be selected from Madison County government officials and staff, Federal and State governments, private industry, the military, as well as quasi-public and volunteer

groups trained in emergency services and response. All training and exercises conducted in Madison County will be documented. Training needs will be identified and records maintained for all personnel assigned emergency response duties in a disaster.

6.4 **Annual Exercises** – The EMC will develop, plan, and conduct functional and/or full-scale exercises annually these will incorporate the information from HSEEP, drills and workshops. These exercises will be designed to not only test the Madison County Emergency Operations Plan and subplans, but to train all appropriate officials, emergency response personnel, County employees, and improve the overall emergency response organization and capability of Madison County. Quasi-public and volunteer groups and/or agencies will be encouraged to participate. Deficiencies identified by the exercise will be addressed immediately.

7.0 Authorities – The organizational and operational concepts set forth in the plan are promulgated under the following authorities:

7.1 Federal

7.1.1 The Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended (42 U.S.C.5121, et seq) Implementing regulations in 44 CFR 206.

7.1.2 National Response Framework, October 2019

- **a.** Homeland Security Act of 2002
- **b.** Executive Order 13603 National Defense Resources Preparedness
- **c.** Presidential Policy Directive 8.

7.1.3 Emergency Management and Assistance, Code of Federal Regulations, Title 44.

7.2 State

7.2.1 Commonwealth of Virginia Chapter 3.2 Emergency Services and Disaster Laws.

7.2.2 The Commonwealth of Virginia Emergency Operations Plan, September 2019

8.0 References

8.1 National Response Framework, October 2019.

8.2 CPG 101, Developing and Maintaining Emergency Operations Plans, Version 2, November 1, 2010 – Updated May 1, 2014.

8.3 Local Mitigation Plan Review Guide, October 1, 2011

9.0 Definitions

Agrosecurity – any situation dealing with local agriculture to include: threats and hazard analysis, risk assessment, damage assessment, agriculture roles and responsibilities and pre-planning.

Emergency Operations Center (EOC) - Centrally located government or community building, equipped with communications and emergency power, for coordination of government services, volunteer organizations, and emergency public information.

Emergency Services - The preparation for and the carrying out of functions (other than functions for which military forces are primarily responsible) to prevent, minimize, and repair injury and damage resulting from natural, man-made, or war-caused disasters. These functions include fire fighting, police, medical and health, rescue first aid, warning, communications, evacuation, resource management, plant protection, restoration of public utility services, and other functions related to preserving the public health, safety, and welfare.

Hazardous Materials - Substances and materials in quantities and forms that may pose an unreasonable risk to health and safety or to property when transported in commerce. Hazardous materials include: explosives, radioactive materials, etiologic agents, flammable liquids or solids, combustible liquids or solids, poisons or poisonous gases, oxidizing or corrosive materials, irritants, compressed gases, and hazardous waste (as defined in United States Department of Transportation Regulations).

Local Emergency - The condition declared by the local governing body when, in its judgment, the threat or actual occurrence of a disaster is or threatens to be of sufficient severity and magnitude to warrant coordinated local government action to prevent or alleviate loss of life, property damage, or hardship. A local emergency arising wholly or substantially out of a resource shortage may be declared only by the Governor, upon petition of a local governing body, when he deems the situation to be of sufficient magnitude to warrant coordinated local government action to prevent or alleviate the hardship or suffering threatened or caused thereby.

Local Emergency Planning Committee (LEPC) - Appointed representatives of local government, private industry, businesses, environmental groups, and emergency response organizations charged with meeting the hazardous materials planning requirements of the Superfund Amendments and Reauthorization Act of 1986 (SARA Title III).

Major Disaster - Any natural or man-made disaster in any part of the United States which, in the determination of the President of the United States, is or thereafter determined to be of sufficient severity and magnitude to warrant disaster assistance above and beyond emergency services by the federal government to supplement the efforts and available resources of the several states, local governments, and relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby and is so declared by him.

Man-Made Disaster - Any industrial, nuclear, or transportation accident, explosion, conflagration, power failure, resource shortage, or other condition such as sabotage, oil spills, and other injurious environmental contaminations which threaten or cause damage to property, human suffering, hardship, or loss of life.

Natural Disaster - Any hurricane, tornado, storm, flood, high water, wind-driven water, tidal wave, earthquake, drought, fire, or other natural catastrophe resulting in damage, hardship, suffering, or possible loss of life.

Resource Shortage - The absence, unavailability, or reduced supply of any raw or processed natural resource or any commodities, goods, or services of any kind which bear a substantial relationship to the health, safety, welfare, and economic well-being of the citizens of the Commonwealth.

Severe Weather "Warning" - Severe weather conditions which could cause serious property damage or loss of life have occurred--have been actually observed or reported. For example, a Flash Flood Warning means that heavy rains have occurred and low-lying areas are likely to be flooded.

Severe Weather "Watch" - Atmospheric conditions indicate that severe weather is possible, but has not yet occurred (e.g., Hurricane Watch, Flash Flood Watch, Tornado Watch, etc.).

Situation Report, Local - A form which, when completed at the end of each day of local EOC operations, will provide the city or County with an official daily summary of the status of an emergency and of the local emergency response. A copy should be submitted to the State EOC via WebEOC.

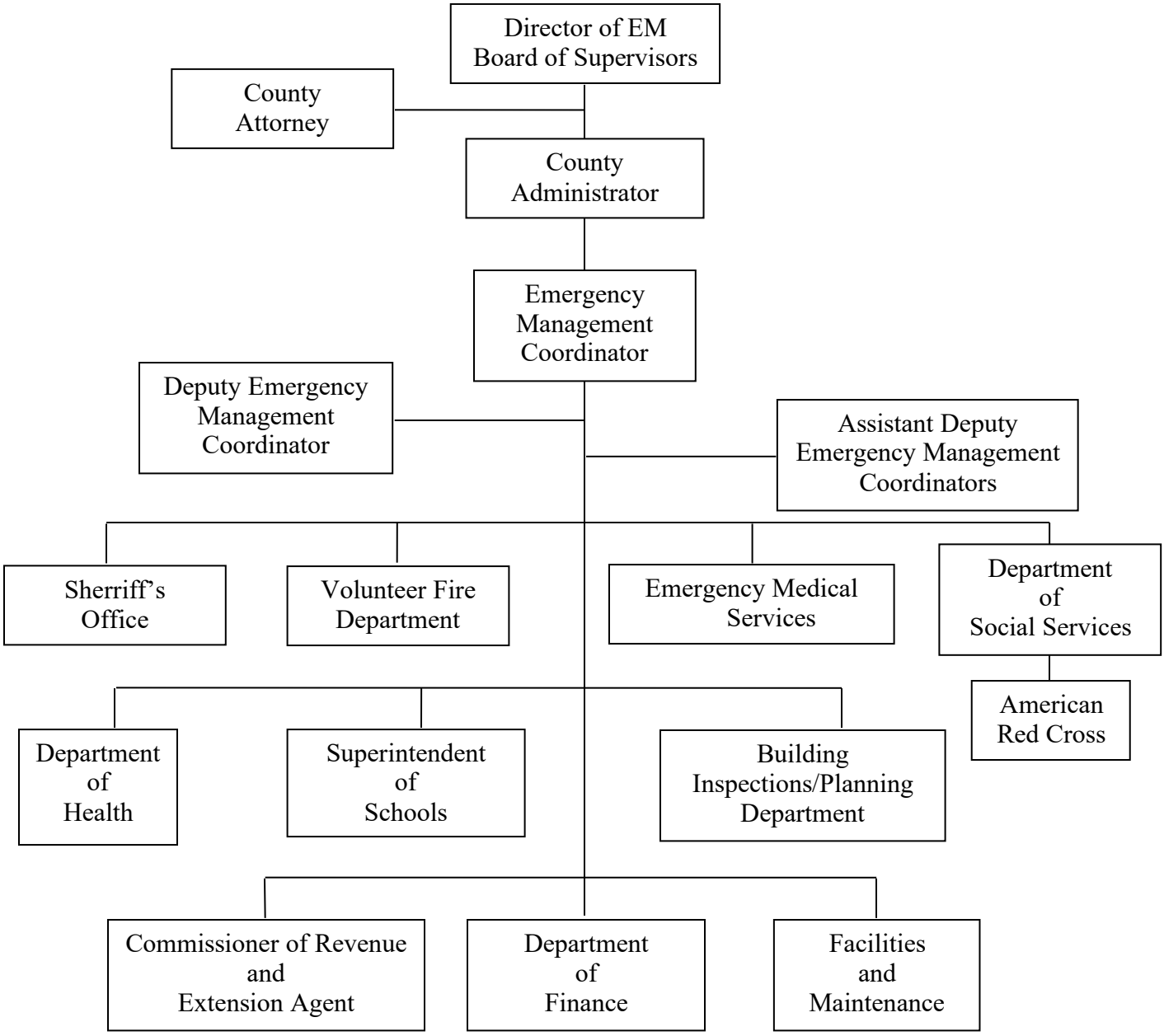
State of Emergency - The condition declared by the Governor when, in his judgment, a threatened or actual disaster in any part of the state is of sufficient severity and magnitude to warrant disaster assistance by the state to supplement local efforts to prevent or alleviate loss of life and property damage.

10.0 Glossary of Acronyms

ARES	Amateur Radio Emergency Service
ACOE	U.S. Army Corps of Engineers
ARC	America Red Cross
BLM	Bureau of Land Management
CAP	Civil Air Patrol
CEM	Comprehensive Emergency Management
CERT	Citizens Emergency Response Team
DAC	Disaster Application Center
DCR	Virginia Department of Conservation and Recreation
DEQ	Virginia Department of Environmental Quality
DFIRM	Digital Food Insurance Rate Map
DHS	Department of Homeland Security
DOF	Virginia Department of Forestry
DOH	Virginia Department of Health
EBS	Emergency Broadcast System
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
EPA	U.S. Environmental Protection Agency
FBI	Federal Bureau of Investigations
FEMA	Federal Emergency Management Agency
GIS	Geographic Information System
HAZMAT	Hazardous Material
HMERP	Hazardous Material Emergency Response Plan
HMO	Hazardous Materials Officer
IA	Individual Assistance
IEMS	Integrated Emergency Management System
LEPC	Local Emergency Planning Committee
MAA	Mutual Aid Agreement
MOA	Memorandum of Understanding
MEDEVAC	Medical Evacuation
MSDS	Material Safety Data Sheets
NOAA	National Oceanic and Atmospheric Administration
NPS	National Park Service
NWS	National Weather Service
PIO	Public Information Officer
RACES	Radio Amateur Civil Emergency Services
SARA	Superfund Amendments and Reauthorization Act
SHMO	State Hazard Mitigation Officer
SMA	Statewide Mutual Aid
SOP	Standing Operating Procedures
VDEM	Virginia Department of Emergency Management
VDOT	Virginia Department of Transportation
VOAD	Volunteer Organizations Active in Disaster
WMD	Weapons of Mass Destruction

Attachment 1

Emergency Management Organization Chart



Attachment 2

Matrix of Responsibilities

O- - Primary responsibility **X**- - Secondary responsibility	Deputy Emergency Manage. Coord.	Emergency Management Coord.	County Administrator	Board of Sup./Director of E.M.	Sheriff ' s Office	Director of E911 Center	Volunteer Fire Department	Emergency Medical Services	Superintendent of Schools	Department of Social Services	Health Department	Facilities/Maintenance	Building Inspections/Planning Dept	County Attorney	Finance Department	County Clerk	Ext. Service/Com. of Revenue	VA Dept. of Transportation	RACES/ARES	American Red Cross	State and Special Police Forces
Direction and Control	**X**	**O**	**X**	**X**										**X**							
Emergency Public Information		**X**	**O**	**X**		**X**															
Law Enforcement					**O**																**X**
Traffic Control					**O**													**X**			**X**
Communications	**X**	**X**			**X**	**O**													**X**		
Warning and Alerting	**X**	**X**			**O**	**X**	**X**	**X**													**X**
Fire Response		**X**					**O**														
Hazardous Materials Response		**X**			**X**		**O**	**X**													
Search and Rescue		**X**			**O**		**X**	**X**													
Evacuation		**X**			**O**		**X**	**X**	**X**												**X**
Radiological Incident Response		**X**					**O**				**X**										
Shelter Operation									**X**	**O**										**X**	
Emergency Medical Transport								**O**													
Mass Feeding									**O**	**X**										**X**	
Welfare Services										**O**	**X**									**X**	
Health Services											**O**										
Utilities Services											**X**	**O**									
Street Maintenance												**O**						**X**			
Debris Removal												**O**						**X**			
Damage Assessment		**X**											**O**		**X**		**X**				
Resource and Supply												**O**			**X**						
Recovery Operations	**X**	**O**	**X**	**X**						**X**	**X**	**X**	**X**	**X**	**X**						
Medical Services								**O**			**X**									**X**	
Mortuary Services								**X**			**O**										
Financial Management/Records	**X**	**X**	**X**												**O**	**X**					

Attachment 3

Sample Resolution for the Declaration of a Local Emergency

WHEREAS, the Board of Supervisors of Madison County does hereby find that:

1. Due to the heavy rain and windstorms, Madison County is facing dangerous flood conditions;

2. Due to the floods, a condition of extreme peril of life and property necessitates the proclamation of the existence of an emergency;

NOW, THEREFORE, IT IS HEREBY PROCLAIMED that an emergency now exists throughout said County and

IT IS FURTHER PROCLAIMED AND ORDERED that during the existence of said emergency the powers, functions, and duties of the Director of Emergency Management and the _____ organization of Madison County shall be those prescribed by state law and the ordinances, resolutions, and approved plans of Madison County in order to mitigate the effects of said emergency.

Dated: _____

Board of Supervisors
Madison County

_____

_____

_____

Attest: _____
Clerk, Board of Supervisors
Madison County
Commonwealth of Virginia

Attachment 4

Emergency Operations Plan Distribution List

Agency/Official	Number of Copies
Emergency Management Director	1
Emergency Management Coordinator	2
Deputy Emergency Management Coordinator	1
Asst. Deputy Emergency Management Coordinators	3
County Administrator	1
Board of Supervisors	5
Sheriff's Office	1
E-911 Communications Center	1
Fire Company	1
Madison Emergency Medical Services	1
School Board	1
Social Services	1
Health Department	1
Facilities/Maintenance	1
Inspections/Engineering	1
Zoning Administrator	1
Emergency Operations Center	1
Extension Service	1
Virginia Department of Transportation	1
Adjacent Counties:	
Orange County	1
Greene County	1
Page County	1
Culpeper County	1
Rappahannock County	1

Attachment 5

List of Information to be Updated Annually

Basic Plan	4.2.2 State Agencies
ESF 1	Tab 1 Transportation Resources for Evacuation Tab 2 Special Transportation Resources
ESF 3	Tab 1 Public Service Corporations Tab 3 Engineering, Inspections, Planning, and Zoning Resources
ESF 4	Tab 1 Fire Department Resources
ESF 5	Tab 1 Emergency Management Organization and Telephone Listing
ESF 6	Tab 2 Special Transportation Resources Tab 3 Madison County Designated Shelters
ESF 7	Tab 1 Facilities and Maintenance Organization and Resources Tab 2 Public Service Corporations Tab 4 Resource List
ESF 8	Tab 1 Health, Medical, and Rescue Resources Tab 2 Commonwealth of Virginia MEDEVAC Services
ESF 13	Tab 1 Law Enforcement Resources Tab 2 Traffic Control Points – Critical Intersections Tab 3 Evacuation Road Networks
ESF 15	Tab 1 Emergency Public Information Resources
SA 3	Tab 2 Hazard Analysis
SA 4	Tab 1 Special Facilities
HSA 1	Tab A Areas Subject to Flooding
HSA 2	Tab B Exhibit 2: Resource Inventory and Index Tab C Special Facilities Tab F Exhibit 1: Hazardous Materials Facilities
HSA 4	Tab A Madison County Dams

Oath of Office.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Commonwealth of Virginia, County of Madison, to-wit:

I, _____, do solemnly swear (or affirm) that I will support the Constitution of the United States, and the Constitution of the Commonwealth of Virginia, and that I will faithfully and impartially discharge all the duties incumbent upon me as a_____

_____,

according to the best of my ability, (So help me God.)

_____

I, _____ Clerk/Deputy Clerk in and for the County of Madison, do certify that _____ This _____ day of _____, 2022, personally appeared before me in my office aforesaid and took and subscribed the above oath.

_____
Clerk

_____
Deputy Clerk

MCSO LEOSA Waiver Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Madison County Sheriff's Office
Release and Waiver of Liability

I, _____ _____, my agents, assigns, executors, or administrators and as a former law enforcement officer eligible for the Federal Law Enforcement Officer Safety Act (LEOSA) SR926b certification, for the consideration of being allowed to enter, and use the Madison County Sheriff's Office Firing Range, firearms and services of the Office, and for other valuable consideration, do hereby absolutely and unequivocally agree to release and hold harmless Madison County, it's agents, officers, employees, instructors, assigns and successors from an claim, demand or liability, whether claimed by myself or another, arising out of any injury, loss or disability connected with the use of these facilities and services. It is the express intent of this Release and Waiver of Liability that the Sheriffs Office, or Madison County will not be responsible for any negligence or other liability and that all risks involved in connection with the use of the premises, whether known or unknown, are expressly assumed by the user.

This waiver includes, but is not limited to the following:

- Bullet ricochets and/or "splash backs". Splash backs are bullets that hit steel or other hard surfaces and fragment. The fragments fly back toward the firing line and may cause bodily harm if it strikes a shooter or observer.
- A defective bullet or firearm may blow up in a shooter's face or hand, causing injury
- Observe and obey all safety rules - Unsafe shooters may kill or injure anyone at any time.

By signing below. I certify that I have read, understand and agree to abided by the RANGE RULES AND RELEASE WAIVER. Futher. I acknowledge that / am not under the influence of drugs or alcohoL and that I have been offered free use of eye and ear protection.

Signature_____ Date: _____

Print: _____ Range Results: Pass_____ Fail_____

Printed Name requested on Card: _____

Mailing Address:(Street)_____ City__ _____Zip_____

317 Virginia Missing Child with Autism Agency Termination Request Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Virginia "Missing Child with Autism Alert" Termination Form

We are terminating the "Missing Child with Autism Alert" originated by our agency. Please broadcast the following information as necessary.

Text Follows

The "Missing Child with Autism Alert" which was transmitted earlier for

(Full name) _____ , missing from

(Street) _____

(City or County) _____ , has been

canceled. The "Autism Alert" for (Full name) _____

has been cancelled.

_____

If there are any problems with or questions about the contents of this fax, call

at

_____ _____

(*NAME*) (*PHONE*)

Text Ends

Originating Agency: _____

317 Virginia Missing Child with Autism Agency Activation Request Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Virginia "Missing Child with Autism Alert" Request Form

Incident Information

Date Missing: _____ (mm/dd/yy) **Time Reported Missing:** _____ (hh:mm)

Location of Incident - last known location:

_____
(Description)

Direction of Travel/Destination:

_____
(City, State, Subdivision)

Vehicle Description:

_____
(Make, Model, Year, Color, License Plate Number and State of Issue)

Childs Information

Name: _____
(Last, First, MI)

Gender: _____ (Male/Female) **DOB:** _____ (mm/dd/yy or Approx. Year) **Race:** _____ (Include all Types)

Height: _____ (Feet/Inches) **Weight:** _____ (Lbs.) **Hair:** _____ (Style and Color) **Eyes:** _____ (Color)

Clothing:

Shirt: _____
(Type, Long or Short Sleeve, Color)

Pants: _____
(Type and Color)

Shoes: _____
(Type and Color)

Other: _____
(Type and Color)

Outerwear: _____
(Type and Color)

Additional Significant Identifiers: _____

_____

Medical Needs: _____

OBTAIN A PHOTOGRAPH OF THE CHILD, AND E-MAIL TO THE VIRGINIA MISSING CHILDREN INFORMATION CLEARINGHOUSE vamissing@vsp.virginia.gov and dutysgthq@vsp.virginia.gov.

Virginia "Missing Child with Autism Alert" Request Form

CONTACT ORGANIZATION:

Sheriff's Office or Police Department: _____

Contact Person: _____

Telephone Number: _____ **Facsimile Number:** _____

Pager Number: _____ **Cellular Telephone Number:** _____

Date and Time Submitted: _____

Virginia "Missing Child with Autism Alert" Request Form

AUTHORIZATION FOR RELEASE OF CHILDS INFORMATION

For a period of one year from the execution of this form, the undersigned authorizes full disclosure of all records concerning my child to any agent of the state of Virginia, Virginia State Police, or any individual or entity assigned by the Virginia State Police, whether the records are of a public, private, internal, or confidential nature. I direct the release of such information regardless of any agreement I may have made to the contrary with any entity or individual to whom my child's information is released or presented. The intent of this authorization is to give my consent for full and complete disclosure of potentially confidential information. Additionally, I understand the duty of the Virginia State Police to release any information to the proper authorities and make other reports as may be mandated by law. I also certify that any person(s) who may furnish such information concerning the my child shall not be held accountable for giving this information; and I do hereby release such person(s) from any and all liability which may be incurred as a result of furnishing such information. I further release the Virginia State Police, Virginia Broadcasters Association and its agents, and designees under this release, from any and all liability which may be incurred as a result of furnishing such information. A photocopy of this release form will be valid as an original thereof, even though the said photocopy does not contain an original writing of my signature. I have read and fully understand the contents of this "Authorization for Release of Information."

PLEASE PRINT OR TYPE:

_____

Last Name, First Name, Middle Initial

_____

Current Address, House Number/Box Number Street Name/Rural Route, City, State, Zip Code

Signature _____

LIABILITY AGREEMENT:

I hereby agree the information I have provided to you acting as an agent of the state of Virginia, Virginia State Police, Virginia Broadcasters Association or any individual or entity assigned by the Virginia State Police, to be truthful, factual, and correct. As the parent/legal custodian, I am aware that in order for the Virginia State Police to activate the Virginia "Missing Child with Autism Alert," the following criteria must be met:

1. The child has been diagnosed with autism spectrum disorder
2. The child is 17 years of age or younger
3. The parent/legal custodian ***must reasonably believe*** the child ***is in danger*** of serious bodily harm or death.

I am also aware I may be charged criminally for committing the crime of knowingly providing false information to law enforcement authorities. I have read and fully understand the contents of this "Liability Agreement."

PLEASE PRINT OR TYPE:

_____

Last Name, First Name, Middle Initial

_____

Current Address, House Number/Box Number Street Name/Rural Route, City, State, Zip Code

Signature: _____

317 Virginia Ashanti Alert - Abducted Adult - Termination Fax Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Virginia Ashanti Alert Termination Fax Form

The enclosed fax is a request for termination of the Virginia Ashanti Alert.

It includes the standard termination text.

There are (*number*)_____ **pages, including this cover sheet.**

The originating agency is (*agency*) _____.

The terminating officer is (*name and title*) _____.

If there are any problems with or questions about the contents of this fax, call (*name*)_____, at (*phone*) _____.

317 Virginia Ashanti Alert - Abducted Adult - Activation Request Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Virginia Ashanti Alert Form

ABDUCTION INFORMATION

Date Abducted: _____ **Time Abducted:** _____
(mm/dd/yy) (hh:mm)

Location of Abduction:

_____
(Description)

Direction of Travel/Destination:_____
(City, State, Subdivision)

Vehicle Description:

_____
(Make, Model, Year, Color, License Plate Number and State of Issue)

ADULT INFORMATION (Complete an additional page for each adult abducted)

Name: _____
(Last, First, MI)

Gender:_____ **DOB:** _____ **Race:** _____
(Male/Female) (mm/dd/yy or Approx. Year) (Include all Types)

Height: _____ **Weight:** _____ **Hair:** _____ **Eyes:** _____
(Feet/Inches) (lbs.) (Style and Color) (Color)

Clothing:

Shirt:

_____
(Type, Long or Short Sleeve, Color)

Pants:

_____
(Type and Color)

Shoes:

_____
(Type and Color)

Other:_____
(Type and Color)

Outerwear:

_____
(Type and Color)

Additional Significant Identifiers:

_____
_____
_____

OBTAIN A PHOTOGRAPH OF THE ADULT, AND E-MAIL TO THE VIRGINIA MISSING PERSONS INFORMATION CLEARINGHOUSE vamissing@vsp.virginia.gov.

Details:

_____
_____

Virginia Ashanti Alert Form

ABDUCTOR INFORMATION (Complete an additional page for each additional abductor)

Name: _____
(Last, First, MI)

Gender:_____ (Male/Female) **DOB:** _____ (mm/dd/yy or Approx. Year) **Race:** _____ (Include all Types)

Height: _____ (Feet/Inches) **Weight:** _____ (lbs.) **Hair:** _____ (Style and Color) **Eyes:** _____ (Color)

Clothing:

Shirt:
_____
_
(Type, Long or Short Sleeve, Color)

Pants:
_____
_
(Type and Color)

Shoes:
_____
_
(Type and Color)

Other:_____
(Type and Color)

Outerwear:_____
(Type and Color)

Additional Significant Identifiers:
_____
_____

Details: _____
_____

CONTACT ORGANIZATION:

Sheriff's Office or Police Department:
_____

Contact Person: _____

Telephone Number: _____ **Facsimile Number:** _____

Pager Number: _____ **Cellular Telephone Number:** _____

Date and Time Submitted:
_____

Virginia Ashanti Alert Form

AUTHORIZATION FOR RELEASE OF MISSING ADULT INFORMATION

For a period of one year from the execution of this form, the undersigned authorizes full disclosure of all records concerning the missing adult to any agent of the Commonwealth of Virginia, Virginia State Police, or any individual or entity assigned by the Virginia State Police, whether the records are of a public, private, internal, or confidential nature, I direct the release of such information regardless of any agreement I may have made to the contrary with any entity or individual to whom the missing adult's information is released or presented. The intent of this authorization is to give my consent for full and complete disclosure of potentially confidential information. Additionally, I understand the duty of the Virginia State Police to release any information to the proper authorities and make other reports as may be mandated by law. I also certify that any person(s) who may furnish such information concerning the missing adult shall not be held accountable for giving this information, and I do hereby release such person(s) from any and all liability which may be incurred as a result of furnishing such information. I further release the Virginia State Police, Virginia Broadcasters Association and its agents, and designees under this release, from any and all liability which may be incurred as a result of furnishing such information. A photocopy of this release form will be valid as an original thereof, even though the said photocopy does not contain an original writing of my signature. I have read and fully understand the contents of the "Authorization for Release of Missing Adult Information."

PLEASE PRINT OR TYPE:

_____

Last Name, First Name, Middle Initial

_____

Current Address, House Number/Box Number Street Name/Rural Route, City, State, Zip Code

Signature:

_____

LIABILITY AGREEMENT:

I hereby agree the information I have provided to you acting as an agent of the Commonwealth of Virginia, Virginia State Police, Virginia Broadcasters Association or any individual or entity assigned by the Virginia State Police, to be truthful, factual, and correct. As the next of kin custodian, I am aware that in order for the Virginia State Police to activate the Virginia Ashanti Alert, the following criteria must be met:

1. The adult is 18 years of age or older,
2. The investigating agency believes the missing adult has been ***abducted***, and
3. The investigating agency believes the adult ***is in danger*** of serious bodily harm or death.

I am also aware I may be charged criminally for knowingly providing false information to law enforcement authorities. I have read and fully understand the contents of this "Liability Agreement."

PLEASE PRINT OR TYPE:

_____

Last Name, First Name, Middle Initial

_____

Current Address, House Number/Box Number Street Name/Rural Route, City, State, Zip Code

Signature: _____

Virginia Ashanti Alert Activation Fax Form

The enclosed fax is a request for activation of the Virginia Ashanti Alert." It includes the standard activation text.

There are (*number*) _____ **pages, including this cover sheet.**

The originating agency is (*Agency*) _____.

The activating officer is (*Name and Title*)

_____

.

UNLESS TERMINATED EARLIER, THIS ALERT WILL AUTOMATICALLY END AT _____.
(*12 hours from current time.*)

If there are any problems with or questions about the contents of this fax, call (*Name*) _____, at (*phone*) _____.

317 Virginia Ashanti Alert - Abducted Adult - Plan.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

VIRGINIA STATE POLICE



ASHANTI ALERT

FOR ABDUCTED ADULTS

APPROVED BY: _____ **DATE:** _____

Colonel Gary W. Settle

TABLE OF CONTENTS

	Page
Summary	1
Definitions	1
Major Components of the Virginia Ashanti Alert System	2
Secondary Components of the Virginia Ashanti Alert System	3
Criteria for the Activation of the Plan	4
Law Enforcement Agency Request Process	5
Activation Process	6
Local Law Enforcement Agencies Responsibilities and Procedures	7
Virginia Missing Persons Clearinghouse Responsibilities and Procedures	8
Virginia Ashanti Alert Activation Flow Chart	10
Appendix A. Virginia Ashanti Alert Forms:	
Virginia Ashanti Alert Form	12
Virginia Ashanti Alert Activation Fax Form	15
Virginia Ashanti Alert Termination Fax Form	16

SUMMARY

The Virginia Ashanti Alert for Abducted Adults (Ashanti Alert) Plan provides a valuable tool for Virginia law enforcement agencies in the ongoing effort to protect our citizens, while allowing the broadcasters of Virginia, the Virginia Department of Transportation, and other partners an opportunity to contribute to the communities they serve in an extremely beneficial capacity.

This plan is available for use by all Virginia law enforcement agencies and can be used as their primary Ashanti Alert Plan or as a supplement to their existing plan.

Definitions:

Ashanti Alert means an adult (i) whose whereabouts are unknown, (ii) who is believed to have been abducted, (iii) who is 18 years of age or older, and (iv) whose disappearance poses a credible threat as determined by law enforcement to the safety and health of the adult and under such other circumstances as deemed appropriate by the Virginia State Police. (Note: See Ashanti Alert Criteria for appropriate circumstances on page 5.)

Ashanti Alert Agreement" means the voluntary agreement between law-enforcement officials and members of the media whereby an adult will be declared abducted, and the public will be notified, and includes all other incidental conditions of the partnership as found appropriate by the Virginia State Police.

Ashanti Alert means the notice of an adult abduction provided to the public by the media or other methods and under an Ashanti Alert Agreement.

Ashanti “Alert Program" or "Program" means the procedures and Ashanti Alert Agreements to aid in the identification and location of Critically Missing Adult.

"Media" means print, radio, television, and internet-based communication systems or other methods of communicating information to the public.

Major Components of the Ashanti Alert System

- **Virginia Criminal Information Network (VCIN)**

  VCIN is a telecommunication system which provides 24-hour access to Virginia law enforcement agencies to enter and query criminal justice information, including information regarding abduction or any matter dealing with missing persons.

- **Virginia Department of Transportation (VDOT) Message Boards and Highway Alert Radio and other VDOT Communication Systems**

  These systems are maintained by VDOT. Electronic changeable message signs and radio systems will be used to disseminate information to the public as they unitize the highway transportation system. Fixed signs are located on major highways throughout the state. If available, these signs and radio system can be used to publicize information regarding abduction. The other communication systems will provide information to Virginia rest areas, welcome centers, truck weigh stations and toll facilities.

- **Virginia Missing Person's Information Clearinghouse (VMPC)**

  The Clearinghouse has the ability to upload photographs and enter information regarding a lost adult on to the Virginia Missing Persons Alert website. Additionally, the VMPC uses Everbridge software to initiate mass messages to media and other partners.

Secondary Components of the Ashanti Alert System

- **Public Utilities' Communication Systems**

  Notification of the major public utilities within the Commonwealth, have communication systems capable of notifying their field employees when the Virginia Ashanti Alert Plan is activated. These utilities include electric companies, gas companies, etc.

- **Notification of a Regional Plan Infrastructure**

  Notification of the coordinator of a regional Ashanti Alert Plan will enable regional plans to notify all those elements of their respective plans, which have not been activated by the Virginia Ashanti Alert Plan.

- **Virginia Realtors Association**

  Notification of the Multiple Listing Services (MLS) will notify the realtors of Virginia when a Virginia Ashanti Alert Plan has been activated.

- **Virginia State Lottery**

  The Virginia State Lottery will display the Ashanti Alert on their lottery machine marquee during activation of the alert. The Marquee used will notify lottery customers of an Ashanti Alert, the location, and for customers to tune to local media or to www.vaseniorалert.com for more details.

- **DMV**

  Ashanti Alert notices are sent to all Customer Service Center location managers. Information provided about the incident is programmed into DMV's Q-Flow queuing system. This information will be set to the TV screens in 73 Customer Service Centers.

Criteria for the Activation of the Plan

1. The Adult must be 18 years of age or older and the law enforcement agency believes the adult has been abducted (unwillingly taken from their environment without permission).
2. The law enforcement agency believes the Adult is in imminent danger of serious bodily harm or death.
3. A law enforcement investigation has taken place that verified the abduction or eliminated alternative explanations.
4. Sufficient information is available to disseminate to the public that could assist in locating the Adult, suspect, and/or the suspect's vehicle.
5. The Adult must be entered into the Virginia Criminal Information Network (VCIN) and the National Crime Information Center (NCIC) missing person files.
6. The Virginia Ashanti Alert Form authorizing release of information must be signed.

Note

If all of the aforementioned criteria are not met, the Virginia Ashanti Alert Plan will not be activated.

Law Enforcement Agency Request Process

The following requirements must be met by the requesting law enforcement agencies. Meeting the established requirements will enable the most effective Ashanti Alert.

- Enter the Adult into the VCIN/NCIC systems ("pack the record" with any and all information that may cause a hit or provide leads during a police contact.).
- Have at least one individual designated as the reporting officer.
- Use the criteria as delineated in the flow chart to determine whether to activate the Virginia Ashanti Alert Plan.
- Provide updates as frequently as they become available to the VMPC.
- Have an assigned telephone number capable of rolling over to at least two separate lines to take telephone calls if the Virginia Ashanti Alert Plan is activated.
- Have volunteers or personnel to receive the telephone calls for a minimum of 24- hours if the plan is activated or until the Alert is canceled.
- Submit the required information through the Virginia Ashanti Alert Activation website to the Virginia Missing Person's Information Clearinghouse immediately upon the initiation of the abduction investigation or as the investigation is developing.
- Submit a photograph of the Missing Adult in JPEG format to the Virginia State Police Duty Sergeant dutysgthq@vsp.virginia.gov.
- Use the termination script in the event the incident is terminated before the 12- hour cycle is over.

ACTIVATION PROCESS

Activation of the Virginia Ashanti Alert Plan will only be initiated through the Virginia State Police. Once the contacted agency receives a report that an adult has been abducted, the following process should be followed:

1. Confirm that abduction has taken place and the criteria have been met.

2. The information submitted through the Ashanti Alert request activation website will be verified with the investigating agency. If the website is unavailable, Virginia Ashanti Alert activation forms, equivalent Regional Plan or Agency forms which contain the required information as set forth in the Virginia Ashanti Alert Plan may be submitted by fax or email.

3. Include a current photograph of the Missing Adult that can be emailed to the State Police duty sergeant.

4. Send the forms to the Virginia Missing Persons Information Clearinghouse (VMPC) by telephonic facsimile. Contact the VMPC immediately confirming receipt of the packet information or if you should have any difficulties transmitting information. Designate a department contact for VMPC (include a name and telephone number on the standardized facsimile form). Local law enforcement agencies must follow intra-departmental policy regarding the actual investigation process involving any abducted/kidnapped adult incident which takes place within their jurisdiction. If a current portrait of the adult is available, forward it along with a copy of all abduction details or summaries to the Virginia Missing Persons Clearinghouse Coordinator at email vamissing@vsp.virginia.gov.

   Telephone #: 804-674-2026 | Facsimile 804-674-6704

5. After being contacted by the reporting agency, VMPC will conduct the required tasks as outlined in this plan and confirm receipt of the Virginia Ashanti Alert information with the reporting agency.

6. After being contacted, the Virginia State Police will contact any/all broadcasting companies through the Everbridge Software. The Virginia State Police may provide supplemental information with a detailed summary of the adult abduction, and forward a copy of the Adult portrait to any/all broadcasting companies.

The above-mentioned steps provide an efficient and streamlined approach to disseminate detailed information regarding a Critically Missing Adult whose life may be in danger. The goal of this notification process is to be quick, clear, concise, uncluttered, and effective.

Local Law Enforcement Agencies' Responsibilities and Procedures

Prior to activation of any Ashanti Alert the Virginia Missing Persons Clearinghouse (VMPC) shall be contacted with the required information to activate the Virginia Ashanti Alert Plan. The requesting agency will be required to submit updated information and notify VMPC of the recovery of the adult or cancellation of the alert.

Law enforcement agencies should follow these operating procedures:

After local law enforcement officials determine an abduction has occurred (Please refer to the Virginia Ashanti Alert (Plan Flow Chart, page 10), they should notify the Virginia Missing Persons Information Clearinghouse immediately at the Virginia State Police Administrative Headquarters and provide them with the required information by fax or email.

Additionally, the law enforcement agency should do the following:

1. As additional information presents itself, including photographs, the agency shall contact the VMPC immediately with updates so the information can be disseminated to the media.

2. Upon closure of the adult abduction case, immediately notify the VMPC with pertinent information.

The prompt broadcasting of abduction is an integral part of the Virginia Ashanti Alert Plan and our statewide adult protection network. **If it saves the life of only one adult, it is well worth your participation. That one adult may be from your community.**

VIRGINIA MISSING PERSONS CLEARINGHOUSE RESPONSIBILITIES AND PROCEDURES

The following procedure is to be used if a Regional Plan has been activated prior to a request for activation of the Virginia Ashanti Alert Plan.

Upon notification that a Regional Plan has been activated, the Virginia Missing Persons Information Clearinghouse (VMPC) shall contact the investigating agency and obtain the required information needed to activate the Virginia Ashanti Alert plan, if requested.

The VMPC shall initiate the required steps to obtain approval as specified below to implement the Virginia Ashanti Alert in order to eliminate a delay in the implementation of the Ashanti Alert if requested by the investigating agency.

The following procedure is to be used if the Virginia Ashanti Alert Plan is being used as the primary plan.

1. Upon receiving a call from a law enforcement agency to activate a Virginia Ashanti Alert, the Virginia Missing Persons Clearinghouse (VMPC) will review the Information request submitted through the Virginia Ashanti Alert request activation website or if not available submit the required forms.

2. The VMPC shall verify that the use of an Ashanti Alert is justified, and will assist the local law enforcement agency with the drafting of an Ashanti Alert Broadcast.

3. The VMPC will immediately notify the CJIS VCIN First Sergeant, CJIS VCIN Administrative Sergeant, or VCIN Lieutenant who will evaluate the request and determine if a Virginia Ashanti Alert should be activated. The VCIN First Sergeant, VCIN Administrative Sergeant, or VCIN Lieutenant will notify the Duty Sergeant of the decision. The CJIS Captain and Executive Staff will be notified by email of the activation.

4. Supervision will then direct the Duty Sergeant to have the VCIN Control Center submit an Ashanti Alert through the Virginia Criminal Information Network (VCIN), activate either statewide or on a regional basis, and activate the VDOT System. Supervision will then ensure that the missing adult is posted onto the VMPC website.

5. Upon activation of the Virginia Ashanti Alert, the VMPC will activate the EAS to broadcast email notices to media and other partners.

VIRGINIA MISSING PERSONS CLEARINGHOUSE RESPONSIBILITIES AND PROCEDURES (CONTINUED)

6. When an Ashanti Alert is activated, the CJIS Division will assist with calls from the media.

7. The VMPC will send a VCIN message to all Virginia criminal justice agencies notifying them that the Virginia Ashanti Alert has been activated and for them to anticipate an increase in their 911-telephone traffic.

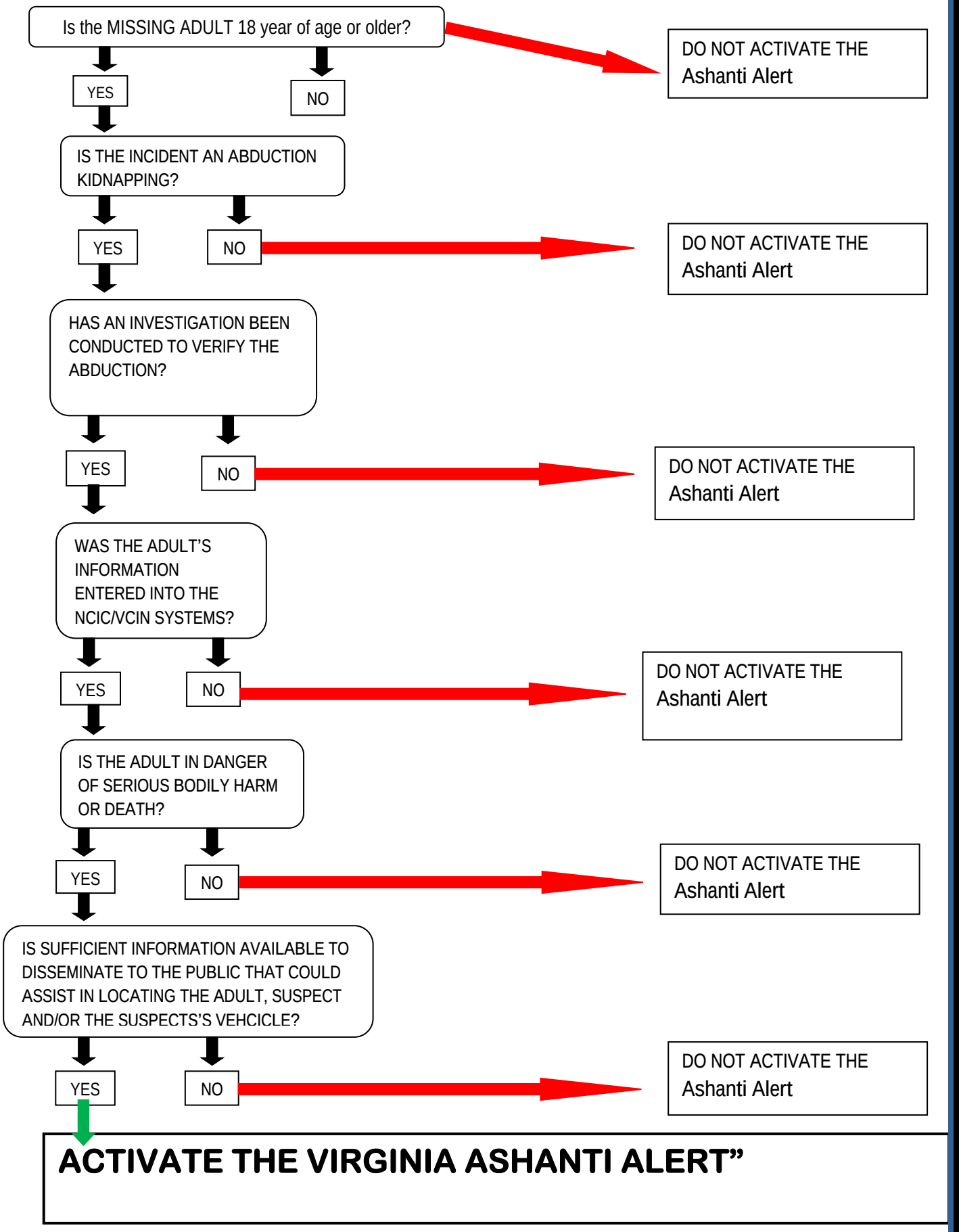
8. The VMPC will coordinate with the agency to determine if assistance is needed in the production of missing person's posters.

9. The VMPC will notify other surrounding states that Virginia has activated the Virginia
   Ashanti Alert plan and provide them with alert information.

Law enforcement agencies are to contact the VMPC immediately if the victim is located, or if the Ashanti Alert should be canceled for some other reason. After receiving this information, VMPC will issue a VCIN cancellation message advising that the Virginia Ashanti Alert has been CANCELED. If the adult was located the message will advise that the Virginia Ashanti Alert has been cancelled – ADULT LOCATED.

Ashanti Alerts are generally approved for 12 hour activation unless new leads or information is obtained to necessitate a time extension. If no additional information is obtained and the alert has been active for 12 hours, VMPC will issue a VCIN cancellation message advising that the Virginia Ashanti Alert has "EXPIRED".

DECISION FLOWCHART FOR VIRGINIA Ashanti Alert PLAN ACTIVATION



APPENDIX
A

VIRGINIA ASHANTI ALERT FORMS

Virginia Ashanti Alert Form

ABDUCTION INFORMATION

Date Abducted: _____ **Time Abducted:** _____
(mm/dd/yy) (hh:mm)

Location of Abduction:

_____
(Description)

Direction of Travel/Destination:_____
(City, State, Subdivision)

Vehicle Description:

_____
(Make, Model, Year, Color, License Plate Number and State of Issue)

ADULT INFORMATION (Complete an additional page for each adult abducted)

Name:

_____
(Last, First, MI)

Gender:_____ **DOB:** _____ **Race:** _____
(Male/Female) (mm/dd/yy or Approx. Year) (Include all Types)

Height: _____ **Weight:** _____ **Hair:** _____ **Eyes:** _____
(Feet/Inches) (lbs.) (Style and Color) (Color)

Clothing:

Shirt: _____
(Type, Long or Short Sleeve, Color)

Pants: _____
(Type and Color)

Shoes: _____
(Type and Color)

Other:_____
(Type and Color)

Outerwear:

_____
(Type and Color)

Additional Significant Identifiers:

_____
_____
_____

OBTAIN A PHOTOGRAPH OF THE ADULT, AND E-MAIL TO THE VIRGINIA MISSING PERSONS INFORMATION CLEARINGHOUSE vamissing@vsp.virginia.gov.

Details:

_____
_____

Virginia Ashanti Alert Form

Page 2

ABDUCTOR INFORMATION (Complete an additional page for each additional abductor)

Name:

_____

(Last, First, MI)

Gender:_____ **DOB:** _____ **Race:** _____

(Male/Female) (mm/dd/yy or Approx. Year) (Include all Types)

Height: _____ **Weight:** _____ **Hair:** _____ **Eyes:** _____

(Feet/Inches) (lbs.) (Style and Color) (Color)

Clothing:

Shirt: _____

(Type, Long or Short Sleeve, Color)

Pants: _____

(Type and Color)

Shoes: _____

(Type and Color)

Other:_____

(Type and Color)

Outerwear:_____

(Type and Color)

Additional Significant Identifiers:

_____

_____

Details: _____

_____

CONTACT ORGANIZATION:

Sheriff's Office or Police Department: _____

Contact Person: _____

Telephone Number: _____ **Facsimile Number:** _____

Pager Number: _____ **Cellular Telephone Number:** _____

Date and Time Submitted:

_____

Virginia Ashanti Alert Form

AUTHORIZATION FOR RELEASE OF MISSING ADULT INFORMATION

For a period of one year from the execution of this form, the undersigned authorizes full disclosure of all records concerning the missing adult to any agent of the Commonwealth of Virginia, Virginia State Police, or any individual or entity assigned by the Virginia State Police, whether the records are of a public, private, internal, or confidential nature, I direct the release of such information regardless of any agreement I may have made to the contrary with any entity or individual to whom the missing adult's information is released or presented. The intent of this authorization is to give my consent for full and complete disclosure of potentially confidential information. Additionally, I understand the duty of the Virginia State Police to release any information to the proper authorities and make other reports as may be mandated by law. I also certify that any person(s) who may furnish such information concerning the missing adult shall not be held accountable for giving this information, and I do hereby release such person(s) from any and all liability which may be incurred as a result of furnishing such information. I further release the Virginia State Police, Virginia Broadcasters Association and its agents, and designees under this release, from any and all liability which may be incurred as a result of furnishing such information. A photocopy of this release form will be valid as an original thereof, even though the said photocopy does not contain an original writing of my signature. I have read and fully understand the contents of the "Authorization for Release of Missing Adult Information."

PLEASE PRINT OR TYPE:

_____

Last Name, First Name, Middle Initial

_____

Current Address, House Number/Box Number Street Name/Rural Route, City, State, Zip Code

Signature: _____

LIABILITY AGREEMENT:

I hereby agree the information I have provided to you acting as an agent of the Commonwealth of Virginia, Virginia State Police, Virginia Broadcasters Association or any individual or entity assigned by the Virginia State Police, to be truthful, factual, and correct. As the next of kin custodian, I am aware that in order for the Virginia State Police to activate the Virginia Ashanti Alert, the following criteria must be met:

1. The adult is 18 years of age or older,
2. The investigating agency believes the missing adult has been ***abducted***, and
3. The investigating agency believes the adult ***is in danger*** of serious bodily harm or death.

I am also aware I may be charged criminally for knowingly providing false information to law enforcement authorities. I have read and fully understand the contents of this "Liability Agreement."

PLEASE PRINT OR TYPE:

_____

Last Name, First Name, Middle Initial

_____

Current Address, House Number/Box Number Street Name/Rural Route, City, State, Zip Code

Signature: _____

Virginia Ashanti Alert Activation Fax Form

The enclosed fax is a request for activation of the Virginia Ashanti Alert." It includes the standard activation text.

There are (*number*) _____ **pages, including this cover sheet.**

The originating agency is (*Agency*) _____.

The activating officer is (*Name and Title*) _____.

UNLESS TERMINATED EARLIER, THIS ALERT WILL AUTOMATICALLY END AT _____.
(*12 hours from current time.*)

If there are any problems with or questions about the contents of this fax, call (*Name*) _____, at (*phone*) _____.

Virginia Ashanti Alert Termination Fax Form

The enclosed fax is a request for termination of the Virginia Ashanti Alert.

It includes the standard termination text.

There are (*number*)_____ **pages, including this cover sheet.**

The originating agency is (*agency*) _____.

The terminating officer is (*name and title*) _____.

If there are any problems with or questions about the contents of this fax, call (*name*)_____, at (*phone*) _____.

317 Virginia AMBER Alert Plan (Rev. 3-1-21).pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

VIRGINIA



AMBER ALERT PLAN

Revised 3-1-21

TABLE OF CONTENTS

	Page
Summary	1
Virginia "AMBER Alert" Advisory Board	2
Major Components of the Virginia "AMBER Alert" System	3
Secondary Components of the Virginia "AMBER Alert" System	4
Wireless Emergency Alert	5
Criteria for the Activation of the Plan	6
Law Enforcement Agency Request Process	7
Activation Process	8
Local Law Enforcement Agencies Responsibilities and Procedures	9
Virginia Missing Children Clearinghouse Responsibilities and Procedures	10-12
Virginia Department of Transportation Responsibilities and Procedures	13
Virginia Lottery and Virginia Department of Transportation	14-15
Virginia Broadcasters Responsibilities and Procedures	16
Cancellation of the Alert/Locating the Child	17
Virginia "AMBER Alert" Activation Flow Chart	18
Appendix A. Virginia "AMBER Alert" Forms:	19
Virginia "AMBER Alert" Form	20-22
Emergency Alert System (EAS) Broadcast Form	23
Virginia "AMBER Alert" Activation Fax Form	24
Virginia "AMBER Alert" Termination Fax Form	25
Virginia "AMBER Alert" Termination Form for EAS	26
Virginia "AMBER Alert" Information Update Form	27

TABLE OF CONTENTS - CONTINUED

Appendix B.	VCIN Virginia "AMBER Alert" Message Formats:	28
	VCIN Agency Virginia "AMBER Alert" Activation Message	29
	VCIN Agency Virginia "AMBER Alert" Cancellation Message	30
Appendix C.	Emergency Alert System (EAS) Local Areas	31-35
Appendix D.	Missing Endangered Child Alert	36-37

SUMMARY

The Virginia "AMBER Alert" (VAA) Plan provides a valuable tool for Virginia law enforcement agencies in the ongoing battle to protect our children, while allowing the broadcasters of Virginia, the Virginia Department of Transportation, and other partners an opportunity to contribute to the communities they serve in an extremely beneficial capacity.

According to the National Center for Missing and Exploited Children (NCMEC), established "AMBER Alert" plans have already been responsible for the recovery of over 602 children nationwide. We are hopeful that Virginia's "AMBER Alert" Plan will not only assist in recovering abducted and endangered children, but also act as a deterrent to this type of crime.

This plan is available for use by all Virginia law enforcement agencies and can be used as their primary "AMBER Alert" Plan or as a supplement to their existing plan.

Definitions:

§52-34.1.

"Abducted child" means a child (i) whose whereabouts are unknown, (ii) who is believed to have been abducted, (iii) who is 17 years of age or younger or is currently enrolled in a secondary school in the Commonwealth, regardless of age, and (iv) whose disappearance poses a credible threat as determined by law enforcement to the safety and health of the child and under such other circumstances as deemed appropriate by the Virginia State Police. (Note: See AMBER Alert Criteria for appropriate circumstances on page 5.)

"Amber Agreement" means the voluntary agreement between law-enforcement officials and members of the media whereby a child will be declared abducted, and the public will be notified, and includes all other incidental conditions of the partnership as found appropriate by the Virginia State Police.

"Amber Alert" means the notice of child abduction provided to the public by the media or other methods and under an Amber Agreement.

"Amber Alert Program" or "Program" means the procedures and Amber Agreements to aid in the identification and location of abducted children.

"Media" means print, radio, television, and Internet-based communication systems or other methods of communicating information to the public.

Virginia's "AMBER Alert" Plan Advisory Board

The Virginia "AMBER Alert" Plan should receive guidance from an Advisory Board consisting of eight members. These members should represent the Department of State Police, the Virginia Association of Chiefs of Police, the Virginia Sheriff's Association, the Virginia Department of Transportation, the Virginia Department of Emergency Management, one individual from the television Cable Systems and two individuals from the Virginia Association of Broadcasters (One member representing radio and one member representing television broadcasters).

Advisory Board Responsibilities and Procedures

The Advisory Board shall attempt to convene a minimum of once a year to review the Virginia "AMBER Alert" Plan.

The Advisory Board shall review and approve all regional plans for the following elements:

- To ensure that each Regional "AMBER Alert" plan contains criteria which are not in conflict with the Virginia "AMBER Alert" Plan.

- To ensure that each Regional "AMBER Alert" Plan contains a requirement that the Virginia Missing Children Information Clearinghouse (VMCC) be notified when a Regional Plan is activated. This requirement will enable the Virginia Missing Children Clearinghouse to contact the investigating agency to obtain the required information to activate the Virginia "AMBER Alert" Plan if requested without delay.

Major Components of the "AMBER Alert" System

- **Emergency Alert System (EAS)**

  EAS is the national civil emergency alert system designed to inform the public of immediate threats to national security, life and property. Employing warning tones, EAS utilizes the public radio/television and broadcast system to share information between public safety agencies and the media; who, in turn, transmit emergency information to the public. The Department of State Police has an Activating terminal to initiate the EAS via Everbridge. Everbridge will be used to send the EAS using the Child Abduction Emergency (CAE) code, and email notifications.

- **Virginia Criminal Information Network (VCIN)**

  VCIN is a telecommunication system which provides 24-hour access to Virginia law enforcement agencies to enter and query information regarding an abduction or any matter dealing with missing children.

- **Virginia Department of Transportation (VDOT) Message Boards and Highway Alert Radio and other VDOT Communication Systems**

  These systems are maintained by VDOT. Electronic changeable message signs and radio systems will be used to disseminate information to the public as they unitize the highway transportation system. Fixed signs are located on major highways throughout the state. If available, these signs and radio system can be used to publicize information to the public regarding a child abduction. The other communication systems will provide information to Virginia Rest Areas, Virginia Welcome Centers, truck weigh stations and toll facilities.

- **Lost Child Alert Technology Resource (LOCATOR) System**

  LOCATOR is a software based system that creates posters of missing children for local, statewide, and national distribution. LOCATOR contains templates for law enforcement agencies to publicize the information to those in the notification lists, during an abduction and when an AMBER Alert is authorized, the Virginia Missing Children Information Clearinghouse (VMCC) ca n create posters for the AMBER Alert. VMCC is the only Virginia agency that can create a LOCATOR poster with the AMBER Alert banner.

- **Virginia Missing Children Information Clearinghouse (VMCC)**

  The Clearinghouse has the ability to upload photographs and enter information regarding a lost child on to the Virginia AMBER Alert website and the National Center for Missing and Exploited Children missing children website. During standard missing children incidents the information can be posted to the state police missing children website.

Secondary Components of the "AMBER Alert" System

- **Public Utilities' Communication Systems**

  Notification of the major public utilities within the Commonwealth which have communication systems capable of notifying their field employees when the Virginia "AMBER Alert" Plan is activated. These utilities include electric companies, gas companies, etc.

- **Notification of a Regional Plan Infrastructure**

  Notification of the coordinator of a regional "AMBER Alert" Plan will enable regional plans to notify all those elements of their respective plans, which have not been activated by the Virginia "AMBER Alert" Plan.

- **Virginia Realtors Association**

  Notification of the Multiple Listing Services (MLS) which will notify the realtors of Virginia when a Virginia "AMBER Alert" Plan has been activated.

- **Virginia State Lottery**

  The Virginia State Lottery will display the Amber Alert on their lottery machine marquee during activation of the alert. The Marquee used will notify lottery customers of an Amber Alert, the location, and for customers to tune to local media or to www.Twitter/VSPalerts.com for more details.

- **A Child Is Missing Program (ACIM)**

  The ACIM program is a non-profit organization that enables law enforcement agencies to create a recorded audio message and publicized by telephone communications. The free service can be used by any law enforcement agency with an executed agreement. The Virginia Missing Person Information Clearinghouse has an agreement with ACIM for using the service. When appropriate during an "AMBER Alert" Alert, the VMCC can contact the organization, identifying affected areas by five zip codes. ACIM will automatically call 1000 telephones numbers in sixty seconds and announce the pre-recorded message regarding the abducted child.

- **DMV**

  Amber Alerts notices are sent to all Customer Service Centers (CSC) location managers. Information provided about the incident is programmed into DMV's Q-Flow Queuing System. This information will be set to the TV screens in 73 Customer Service Centers.

- **WIRELESS EMERGENCY ALERT (WEA)**

AMBER Alerts are distributed to cell phones as part of the AMBER Alert program's secondary distribution through the Wireless Emergency Alert program which is also known as the Commercial Mobile Alert System.

The Wireless Emergency Alert program is operated by the Federal Emergency Management Agency. It distributes notifications from authorized federal, state, local and tribal government agencies that alert customers with capable devices of imminent threats to safety or an emergency situation. The messages are intended as a supplement to the existing Emergency Alert System, which broadcasts alerts over radio and television.

Because the alerts are sent on a special wireless carrier channel called Cell Broadcast they are not affected by congestion on the voice or SMS text channels. The alerts are transmitted simultaneously to all mobile devices within range of the cellular carrier towers in the affected area. The system does not need to know your mobile number and it does not track your whereabouts; it simply broadcasts the alert, and any mobile devices that can "hear" the alert will display it to the user.

The Virginia Missing Children's Clearinghouse will use WEA as a tool to help locate an abducted child. The WEA may be issued by county, division, or along an interstate system. The WEA can use up to 360 characters and will only be used if a vehicle and registration is known, or suspected to be involved in the Virginia Amber Alert activation.

Due to the tone that is given during the activation of a WEA, it will not be activated during midnight hours, unless there is a higher than normal probability that the abducted child is in a small location. Then the WEA may be activated to a specific targeted location. If the abducted child is still missing during the morning hours WEA may be authorized to a broader area.

Criteria for the Activation of the Plan

1. The abducted child must be 17 years of age or younger or is currently enrolled in a secondary school in the Commonwealth, regardless of age,, and the law enforcement agency believes the child has been abducted (unwillingly taken from their environment without permission from the child's parent or legal guardian).

2. The law enforcement agency believes the abducted child is in imminent danger of serious bodily harm or death.

3. A law enforcement investigation has taken place that verified the abduction or eliminated alternative explanations.

4. Sufficient information is available to disseminate to the public that could assist in locating the child, suspect, and/or the suspect's vehicle.

5. The Child must be entered into the Virginia Criminal Information Network (VCIN) and the National Crime Information Center (NCIC) missing person files as soon as practical.

6. The Virginia "Amber Alert" Form authorizing release of information must be signed.

Note

If all of the aforementioned criteria are not met, the Virginia "Amber Alert" Plan will not be activated. However, the Missing Endangered Child Alert may be used.

Law Enforcement Agency Request Process

The following requirements must be met by the requesting law enforcement agencies, Meeting the established requirements will enable the most effective "AMBER" Alert.

- Enter the abducted child into the VCIN/NCIC systems ("pack the record" with any and all information that may cause a hit or provide leads during a police contact.).
- Have at least one individual designated as the reporting officer.
- Use the criteria as delineated in the flow chart to determine whether to activate the Virginia "AMBER Alert" Plan.
- Provide updates as frequently as they become available to the VMCC.
- Have an assigned telephone number capable of rolling over to at least two separate lines to take telephone calls if the Virginia "AMBER Alert" Plan is activated.
- Have volunteers or personnel to receive the telephone calls for a minimum of 24-hours if the plan is activated or until the Alert is canceled.
- Submit the required information through the Virginia AMBER Alert Activation website to the Virginia Missing Children Information Clearinghouse immediately upon the initiation of the abduction investigation or as the investigation is developing.
- Submit a photograph of the abducted child in JPEG format with the website submission.
- Use the termination script in the event the incident is terminated before the 12- hour cycle is over.

ACTIVATION PROCESS

Activation of the Virginia "AMBER Alert" Plan will only be initiated through the Virginia State Police. Once the contacted agency receives a report that a child has been abducted, the following process should be followed:

1. Confirm that an abduction has taken place and the criteria have been met.

2. The information submitted through the AMBER Alert Request Activation website will be verified with the investigating agency. If the website is unavailable, Virginia "AMBER Alert" Activation forms, equivalent Regional Plan or Agency forms which contain the required information as set forth in the Virginia "AMBER Alert" Plan may be submitted.

3. Include a current photograph of the abducted child that can be emailed or submitted through the AMBER Alert Request Activation website.

4. If the website is unavailable, send the forms to the Virginia Missing Children Information Clearinghouse (VMCC) by telephonic facsimile. Contact the VMCC immediately confirming receipt of the packet information, or if you should have any difficulties transmitting information, designate a department contact for VMCC (include a name and telephone number on the standardized facsimile form). Local law enforcement agencies must follow intra-departmental policy regarding the actual investigation process involving any abducted/kidnapped child incident, which takes place within their jurisdiction. If a current portrait of the child is available, forward it along with a copy of all abduction details or summaries to the Virginia Missing Children Clearinghouse Manager vamissing@vsp.virginia.gov and dutysgthq@vsp.virginia.gov.
   Telephone #: 804-674-2026 **Facsimile #: 804-674-6704**

5. After being contacted by the reporting agency, VMCC will conduct the required tasks as outlined in this plan and confirm receipt of the Virginia "AMBER Alert" information with the reporting agency.

6. After being contacted, the Virginia State Police will contact any/all broadcasting companies through the Emergency Alert System (EAS) as per the Virginia Emergency Alert System Plan. The Virginia State Police may provide supplemental information with a detailed summary of the child abduction, and forward a copy of the abducted child's portrait to any/all broadcasting companies. All Virginia Emergency Alert System activations for "AMBER Alert" (CAE) will conform to the Virginia Emergency Alert System Plan.

7. After an initial EAS "AMBER Alert" has been broadcasted, a rebroadcast of "AMBER Alert" information (non-EAS) is made at least every 15 minutes for the first two hours, and every 30 minutes for the next three hours. Once the first five hours have passed, the broadcasters may provide the information and any updates on an hourly basis for the next seven hours (not to exceed 12 hours after the notification was received, unless circumstances dictate that the alert should be extended). The decision to rebroadcast the "AMBER Alert" information will be left up to each individual broadcasting station and is completely voluntary. Only one EAS message will be broadcast.

The above-mentioned steps provide an efficient and streamlined approach to disseminate detailed information regarding an abducted child whose life may be in danger. The goal of this notification process is to be quick, clear, concise, uncluttered, and effective.

Local Law Enforcement Agencies Responsibilities and Procedures

Prior to activation of any "AMBER Alert" the Virginia Missing Children Information Clearinghouse (VMCC) shall be contacted with the required information to activate the Virginia "AMBER Alert" Plan. The requesting agency will be required to submit updated information and notify the VMCC of the recovery of the child or cancellation of the alert.

Law enforcement agencies should follow these operating procedures:

After local law enforcement officials determine an abduction has occurred (Please refer to the Virginia "AMBER Alert" (Plan Flow Chart, page 18), they should notify the Virginia Missing Children Information Clearinghouse immediately at the Virginia State Police Administrative Headquarters and provide them with the required information through the Virginia "AMBER Alert" Request Activation Website.

Additionally, the law enforcement agency should do the following:

1. As additional information presents itself, including photographs, the agency shall contact the VMCC immediately with updates so the information can be disseminated to the media.

2. Upon closure of the child abduction case, immediately notify the VMCC with pertinent information.

The prompt broadcasting of an abduction is an integral part of the Virginia "AMBER Alert" Plan and our statewide child protection network. **If it saves the life of only one child, it is well worth your participation. That one child may be from your community.**

Virginia Missing Children Information Clearinghouse Responsibilities and Procedures

The following procedure is to be used if a Regional Plan has been activated prior to a request for activation of the Virginia "AMBER Alert" Plan.

1. Upon notification that a Regional Plan has been activated, the Virginia Missing Children Information Clearinghouse (VMCC) shall contact the investigating agency and obtain the required information needed to activate the Virginia "AMBER Alert" (VAA) plan, if requested.

2 The VMCC shall initiate the required steps to obtain approval as specified below to implement the Virginia "AMBER Alert" (VAA) in order to eliminate a delay in the implementation of the VAA if requested by the investigating agency.

The following procedure is to be used if the Virginia "AMBER Alert" Plan is being used as the primary plan.

1. Upon receiving a call from a law enforcement agency to activate a Virginia "AMBER Alert" (VAA), the Virginia Missing Children Clearinghouse (VMCC) will review the VAA Information Request submitted through the Virginia "AMBER Alert" Request Activation website or if not available submit the required forms.

2. The VMCC shall verify that the use of an "AMBER Alert" is justified, and will assist the local law enforcement agency with the drafting of a "VAA Broadcast."

3. The VMCC will immediately notify the CJIS VCIN First Sergeant who will notify and confer with the CJIS Lieutenant. They will evaluate the request and determine if a Virginia "Amber Alert" (VAA) should be activated. The VCIN First Sergeant will notify the Duty Sergeant of the decision. The CJIS Lieutenant will then notify the CJIS Captain and Executive Staff.

    a. If the VCIN First Sergeant and CJIS Lieutenant do not agree, the CJIS Captain will be contacted. The CJIS Captains decision will determine if the VAA will be activated.

4. The VCIN First Sergeant will then direct the Duty Sergeant to have the VCIN Control Center to submit a VAA through the Virginia Criminal Information Network (VCIN), activate the Emergency Alert System (EAS) either statewide or on a regional basis, activate the VDOT System, direct the VMCC to have the locater system activated if needed, and provide information to the National Center for Missing and Exploited Children. The Duty Sergeant will then ensure that the missing child is posted onto the VMCC and NCMEC website.

5. Upon activation of the Virginia "AMBER Alert", the VMCC will activate the Everbridge EAS to initiate the EAS broadcast.

Virginia Missing Children Clearinghouse
Responsibilities and Procedures (Continued)

6. When an "AMBER Alert" is activated, the Criminal Justice Information Services Division will assist with calls from the media. The VMCC staff will continue to maintain contact with the Superintendent, Deputy Superintendent, Director or Deputy Director of the Bureau of Administrative Support Services, and the investigating Agency regarding updates and new information.

7. The VMCC will send a VCIN message to all Virginia criminal justice agencies notifying them that the Virginia "AMBER Alert has been activated and for them to anticipate an increase in their 911-telephone traffic.

8. The VMCC will coordinate with the investigating agency to determine if assistance is needed in the production of missing children posters.

9. The VMCC will coordinate having a photograph of the child entered into the National Center for Missing and Exploited Children website.

10. The VMCC will notify other surrounding states that Virginia has activated the Virginia "AMBER Alert" Plan and provide them with alert information.

11. If an "AMBER Alert" is not activated, VMCC may submit information to all participating Virginia media, law enforcement and businesses using the Endangered Missing Child Media Alert.

12. If appropriate, and if the agency is unable to do so, initiate the A Child is Missing Program (ACIM). VMCC personnel will help with the process after obtaining the required information or initiate the ACIM process if requested by the investigating agency.

    The following are the organizations procedure and information required to request and initiate ACIM Program:

    Phone: toll-free 888-875-2246 or 954-763-1288,

    Fax: 954-763-4569

    ACIM takes all pertinent information, including but not limited to:

    - Name of law enforcement agency
    - City, county and state of agency
    - Name of person missing
    - Date of Birth
    - Gender
    - Nationality
    - Height and Weight
    - Hair and Eye color
    - Clothing description
    - Any scars or other physical characteristics
    - Any medical/psychological conditions to be aware of

- Home address including zip code
- Location last seen with zip code if different than residence
- Police department phone number for the public to call to report information
- Case # or Reference # assigned to the case
- If there is water or wooded areas in the vicinity
- Have friends and family been contacted
- Has the child gone missing before
- Is there foul play, kidnapping or parental abduction suspected
- Is the agency aware of any sexual predators or registered sex offenders within 1 mile of the last 1 mile of the location the child was last seen?

A Child Is Missing also requests a cell phone number to reach the **officer on the scene** for additional information. ACIM then makes a recorded message with the information that has been supplied. The location last seen is entered into the computer and a database of phone numbers of the residents/businesses is gathered. The message is then sent out to the community.

When a child is reported missing near water, the immediate area is canvassed with the message, then the search area is expanded if the child has not been found.

ACIM continues to work with the officer on the scene and/or the communications department until the missing person has been found.

After recovery, the agency calls ACIM to stop the search. ACIM then faxes a case follow-up form to the officer/agency to be filled out, documenting the conclusion of the case. The agency then faxes the form back to ACIM. This documentation assists ACIM in obtaining funding to continue offering their services to law enforcement.

Please be sure to advise your Public Information Office about ACIM involvement in searches. This makes for good public relations with the community as the public is made aware that your agency is utilizing all resources possible to ensure their safety.

Law enforcement agencies are to contact the VMCC immediately if the victim is located, or if the "AMBER Alert" should be canceled for some other reason. After receiving this information, VMCC will issue a VCIN Message and VAA cancellation message advising that the Virginia "AMBER Alert" has been CANCELED. If the child was located the message will advise that the Virginia "AMBER Alert" has been cancelled -- CHILD LOCATED.

Amber Alerts are generally approved for 12 hour activation unless new leads or information is obtained to necessitate the time extension. If no additional information is obtained and the alert has timed out VMCC will issue a VCIN Message and VAA cancellation message advising that the Virginia "AMBER Alert" has "EXPIRED".

Virginia Department of Transportation (VDOT) Responsibilities and Procedures

This document serves as Traffic Emergency Operations Center's (TEOC) guidance for VDOT's response to, and reporting of, Virginia "AMBER Alert" requests from the Department of State Police. VDOT is able to quickly disseminate "AMBER Alert" information to the public via our Variable Message Signs (VMS), Highway Alert Radio (HAR), Ticker and Travel Advisory messages. In addition, photos of missing/abducted children may be posted in our Welcome Centers/Rest Areas and distributed to field personnel. The use of messaging signs will be determined on a case by case basis. In the areas of immediate concern VDOT will use display the AMBER ALERT, TAG number and vehicle description. Outside the area of concern, VDOT will display AMBER ALERT, TUNE TO LOCAL MEDIA. (Areas of immediate concern will be determined by the Department of State Police after conferring with the local agency requesting the alert.)

1. If the "AMBER Alert" comes from the Virginia State Police (VSP), proceed immediately to the action steps.

2. If the "AMBER Alert" comes from VDOT field staff (i.e. District Staff, STC), verify that they have received the request from a law enforcement agency. Immediately notify the **VSP SPHQ Duty Sergeant** at **804-674-2026, and determine if the Virginia "AMBER Alert" is being activated.**

WHEN A VIRGINIA "AMBER ALERT" REQUEST IS RECEIVED FROM THE STATE POLICE, THE FOLLOWING STEPS WILL BE TAKEN:

1. Notify the applicable Smart Traffic Center (STC) for the District in which the incident occurred, and/or Virginia Transportation Technical Institute (VTTI). Inform them that we have an "AMBER Alert" request.

   - Advise them of the information received from law enforcement.
   - Instruct them to place a Virginia "AMBER Alert" message on appropriate VMS* and in HAR* (See Appendix D).
   - Confirm the information relayed, and your instructions, by e-mail and to the STC Shift Supervisor and/or VTTI.
   - Be prepared to forward the message to additional districts for VMS and HAR coverage, if the incident is extended.

2. If the law enforcement agency forwarded an "AMBER Alert" bulletin, and/or a photograph of the missing child,

   - E-mail the bulletin/photograph to WELCOME CENTERS, with a request that they post them in a prominent place.
   - Fax/Email the bulletin/photograph to the Rest Areas. Email is the preferred method if a photo is attached.

3. Page EOC WEATHER SITREP with a summary of the Virginia "AMBER Alert" information.

4. Place the Virginia "AMBER Alert" information in the Ticker and Travel Advisory (See Appendix D).

5. Create a High Profile VOIS incident with the Virginia "AMBER Alert" information. Page and e-mail additional people/groups per the Standing Operations Procedure (SOP) pertaining to the affected district.
6. E-mail the "AMBER Alert" information to EOC WEATHER/SITREP and WELCOME CENTERS (See Appendix D).
7. (After hours) Call the Director and the Deputy Director of the Emergency Operations Center and inform them of the "AMBER Alert" information.
8. Be prepared to forward updated information (i.e. law enforcement may discover information about a vehicle used in the abduction) to whomever has been notified.
9. Document everything you have done in the Journal.

* If a serious incident requires the use of the VMS and/or HAR, the agency should run their incident message, as the incident requires. Once the incident is cleared, the agency is to resume running the normal messages.

THE VIRGINIA LOTTERY PROCEDURES

These procedures serve as a guidance for the Virginia Lottery's response to an Amber Alert.

1. Virginia State will fax an alert notification to both fax machines at the Primary Data Center (PDC):
    - 804-228-7782
    - 804-228-7783
2. PDC will immediately update:
    - The VFD message that displays on all Altura terminals; and the message scroll on the Lottery Express devices.
    - The Amber Alert will preempt all other messages.
    - Message text to be entered:
        - AMBER ALERT – City/County Tune to local media or www.Twitter.com/VSPalerts for details.
3. Unless other instructed, PDC will remove Amber Alert message when either:
    - The alert is cancelled by the Virginia State Police.
    - Five (5) hours after the Amber Alert was issued by the Virginia State Police.
4. If an alert notification or cancellation is received from VSP during a time when Lottery retailer devices are not operational (i.e. during overnight processing), the PDC will make the necessary adjustments to Steps 2 and 3 above.
5. PDC will send an informational voice mail and email to all "Active Members" advising them when an Amber Alert notification is received, and when the alert is either cancelled or removed from Lottery devices.

DMV PROCESS

Amber Alert message is received via email from the Virginia Department of State Police by DMV Law Enforcement Services, Assistant Commissioner, and other participants as requested by DMV. When an Amber Alert notice is received it is sent to all Customer Service Center (CSC) location managers to alert them of the Amber Alert. The link to the www.Twitter.com/VSPalerts website is provided so that information about the individual is available to the location managers.

Information provided about the incident is programmed into DMV's Q-Flow Queuing System. This information will be sent to the TV screens in DMV Customer Service Centers. The information will be displayed in a scroll format across the bottom of the TV screen. It will be in a continuous scroll until the alert is cancelled. When notification is received that the alert is cancelled, the CSC's are informed that the alert is cancelled. The Q-Flow TV's are reprogrammed with the regular DMV scroll messages.

VIRGINIA BROADCASTERS

RESPONSIBILITIES AND PROCEDURES

After receiving the EAS Message from the Virginia State Police, the broadcasters can either pass through or transcribe the information included in the EAS Message, faxed or e-mailed Virginia "AMBER Alert" Notification.

After an initial EAS "AMBER Alert" has been broadcasted, it is suggested a rebroadcast of "AMBER Alert" information (non-EAS) is made at least every 15 minutes for the first two hours, and every 30 minutes for the next three hours. Once the first five hours have passed, the broadcasters may provide the information and any updates on an hourly basis for the next seven hours (not to exceed 12 hours after the notification was received, unless circumstances dictate that the alert should be extended). The decision to rebroadcast the "AMBER Alert" information will be left up to each individual broadcasting station, and is completely voluntary.

The Broadcasters will provide their audience with critical information included in the Virginia "AMBER Alert" Plan and other pertinent information that will assist law enforcement in the recovery of the child or identification of a suspect or suspect's vehicle.

Upon the termination of a Virginia "AMBER Alert," the broadcaster will provide information to their audience regarding the cancellation of the Virginia "Amber Alert".

Endangered Missing Child Media Alert:

During certain incidents that may not meet all the AMBER Alert criteria, the VMCC will provide an Endangered Missing Child Media Alert. These alerts will be used in those incidents that raise serious concern for the missing child. Media outlets are encouraged to publicize the information as often as possible to help enable the safe return of the missing child. These incidents will involve those cases where information is limited regarding the suspect, suspect vehicle or when the missing child investigations have not clearly identified that an abduction has occurred or that parents and/or family members are involved in the abduction.

The Media are encouraged to broadcast the information as frequently as an AMBER Alert that may not interrupt broadcasts.

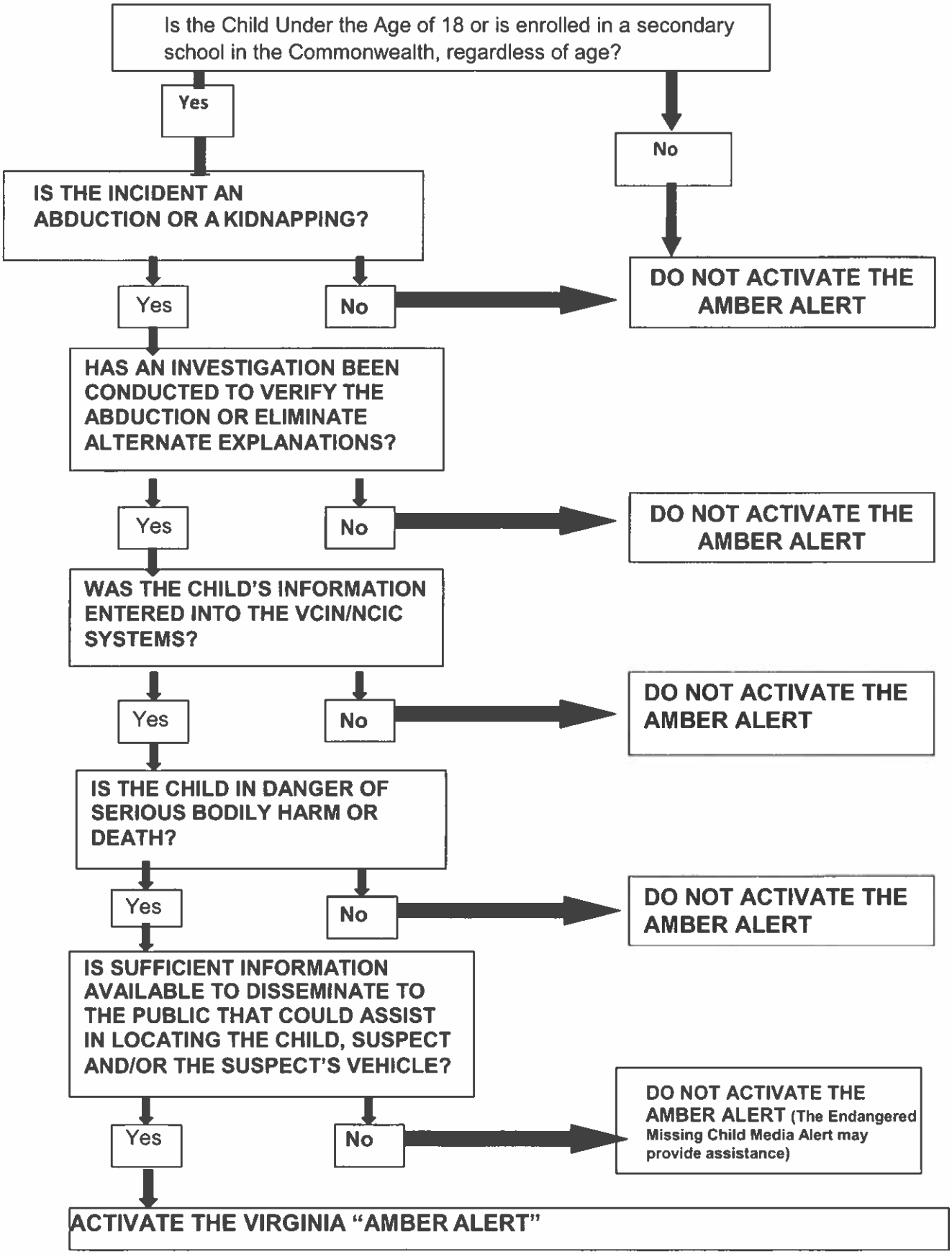
CANCELLATION OF THE ALERT/LOCATING THE CHILD

Subsequent updates shall be provided to the Virginia Missing Children Information Clearinghouse (VMCC) by the investigating agency.

The VMCC must be notified immediately, if the child has been located, or upon closure of the child abduction case. The VMCC will notify all components of the Virginia "AMBER Alert" (VAA) Plan regarding the termination of the VAA.

After the termination of the VAA, any updates may continue to be made directly to the Virginia Missing Children Information Clearinghouse.

DECISION FLOWCHART FOR VIRGINIA "AMBER ALERT" PLAN ACTIVATION



APPENDIX A

VIRGINIA "AMBER ALERT" FORMS

Virginia "AMBER Alert" Form

ABDUCTION INFORMATION

Date Abducted:_____ **Time Abducted:** _____
(mm/dd/yy) (hh:mm)

Location of Abduction: _____
(Description)

Direction of Travel/Destination: _____
(City, State, Subdivision)

Vehicle Description: _____
(Make, Model, Year, Color, License Plate Number and State of Issue)

CHILD INFORMATION (Complete an additional page for each child abducted)

Name: _____
(Last, First, MI)

Gender:_____ **DOB:**_____ **Race:** _____
(Male/Female) (mm/dd/yy or Approx. Year) (Include all Types)

Height:_____ **Weight:**_____ **Hair**_____ **Eyes:** _____
(Feet/Inches) (Lbs.) (Style and Color) (Color)

Clothing:

Shirt: _____
(Type, Long or Short Sleeve, Color)

Pants: _____
(Type and Color)

Shoes: _____
(Type and Color)

Other: _____
(Type and Color)

Outerwear: _____
(Type and Color)

Additional Significant Identifiers:_____

_____

OBTAIN A PHOTOGRAPH OF THE CHILD, AND E-MAIL TO THE VIRGINIA MISSING CHILDREN INFORMATION CLEARINGHOUSE vamissing@vsp.virginia.gov and dutysgthq@vsp.virginia.gov

Details:_____

_____

Virginia "AMBER Alert" Form

ABDUCTOR INFORMATION (Complete an additional page for each additional abductor)

Name: _____
(Last, First, MI)

Gender: _____ **DOB:** _____ **Race:** _____
(Male/Female) (mm/dd/yy or Approx. Year) (Include all Types)

Height: _____ **Weight:** _____
(Feet/Inches) (Lbs)

Hair: _____ **Eyes:** _____
(Style and Color) (Color)

Clothing:
Shirt: _____
(Type, Long or Short Sleeve, Color)

Pants: _____
(Type and Color)

Other: _____
(Type and Color)

Shoes: _____
(Type and Color)

Outerwear: _____
(Type and Color)

Additional Significant Identifiers: _____
_____

Details: _____
_____

CONTACT ORGANIZATION:

Sheriff's Office or Police Department: _____

Contact Person: _____

Telephone Number: _____ **Facsimile Number:** _____

Pager Number: _____ **Cellular Telephone Number:** _____

Date and Time Submitted: _____

Virginia "AMBER Alert" Form

AUTHORIZATION FOR RELEASE OF MISSING CHILD INFORMATION

For a period of one year from the execution of this form, the undersigned authorizes full disclosure of all records concerning my child to any agent of the state of Virginia, Virginia State Police, or any individual or entity assigned by the Virginia State Police, whether the records are of a public, private, internal, or confidential nature. I direct the release of such information regardless of any agreement I may have made to the contrary with any entity or individual to whom my child's information is released or presented. The intent of this authorization is to give my consent for full and complete disclosure of confidential juvenile information. Additionally, I understand the duty of the Virginia State Police to release any information to the proper authorities and make other reports as may be mandated by law. I also certify that any person(s) who may furnish such information concerning my child shall not be held accountable for giving this information; and I do hereby release such person(s) from any and all liability which may be incurred as a result of furnishing such information. I further release the Virginia State Police, Virginia Emergency Management Agency, Virginia Broadcasters Association and its agents, and designees under this release, from any and all liability which may be incurred as a result of furnishing such information. A photocopy of this release form will be valid as an original thereof, even though the said photocopy does not contain an original writing of my signature. I have read and fully understand the contents of this "Authorization for Release of Juvenile Information."

PLEASE PRINT OR TYPE:

_____

Last Name, First Name, Middle Initial

_____

Current Address, House Number/Box Number Street Name/Rural Route, City, State, Zip Code

Signature: _____

LIABILITY AGREEMENT:

I hereby agree the information I have provided to you acting as an agent of the state of Virginia, Virginia State Police, Virginia Broadcasters Association or any individual or entity assigned by the Virginia State Police, to be truthful, factual, and correct. As the parent/legal custodian, I am aware that in order for the Virginia State Police to activate the Virginia "AMBER Alert," the following criteria must be met:

1. The child is 17 years of age or younger, and
2. The parent/legal custodian ***must reasonably believe*** the child ***is in danger*** of serious bodily harm or death.

I am also aware I may be charged criminally for committing the crime of knowingly providing false information to law enforcement authorities. I have read and fully understand the contents of this "Liability Agreement."

PLEASE PRINT OR TYPE:

_____

Last Name, First Name, Middle Initial

_____

Current Address, House Number/Box Number Street Name/Rural Route, City, State, Zip Code

Signature : _____

COMMONWEALTH OF VIRGINIA Emergency

Alert System (EAS) Broadcast Form

(Check one) (Use EAS Operational Map to determine activation areas.)

____REQUEST ADMINISTRATIVE ALERT OR BLAST FAX IN EAS AREAS _____
(Attention Broadcasters: Please read at the next break. Administration Alert will also include a Blast Fax to all stations.)

____REQUEST TONE ALERT IN EAS AREAS _____
(Attention Broadcasters: Please Read Immediately)
(Attention Law Enforcement: To be used only in an immediately known "endangered" Case)
(TONE: Alert will also include a Blast Fax in all stations within the EAS systems.)

Urgent Urgent Urgent Urgent Urgent

THE VIRGINIA STATE POLICE HAS ISSUED AN "AMBER" CHILD ABDUCTION ALERT

FOR AN ABDUCTED CHILD IN _____
(Name of City or County)

THE _____
(Law Enforcement Agency)

AND THE VIRGINIA MISSING CHILDREN CLEARINGHOUSE ARE LOOKING FOR

_____ A_____.
(Child's Name) (Description Sex/Age/Race/Height/Weight/Eyes/Hair)

CHILD WAS LAST SEEN AT_____AND IS
(Location)

BELIEVED TO BE IN EXTREME DANGER. CHILD WAS LAST SEEN WEARING _____

_____
(Clothing Description)

AUTHORITIES SAY THE CHILD WAS LIKELY ABDUCTED BY A _____

_____
(Suspect Description)

THEY/CHILD MAY BE TRAVELING IN A _____
(Vehicle Description, Year, Color, Make, Model and Tag Number)

WHICH WAS LAST SEEN TRAVELING _____
(Direction of Travel)

PLEASE CONTACT_____AT _____
(Local Law Enforcement Agency) (Telephone Number)

OR THE VIRGINIA STATE POLICE AT 1-800-822-4453.
End of Message

Virginia "AMBER Alert" Activation Fax Form

The enclosed fax is a request for activation of the Virginia "AMBER Alert."

It includes the standard activation text.

There are (*number*)_____**pages, including this cover sheet.**

The originating agency is (*Agency*)_____.

The activating officer is (*Name and Title*)_____.

UNLESS TERMINATED EARLIER, THIS ALERT WILL AUTOMATICALLY END AT_____.
(*12 hours from current time.*)

If there are any problems with or questions about the contents of this fax, call (*name*) _____, at (*phone*)_____.

Virginia "AMBER Alert" Termination Fax Form

The enclosed fax is a request for termination of the Virginia "AMBER Alert."

It includes the standard termination text.

There are (*number*)_____**pages, including this cover sheet.**

The originating agency is (*agency*)_____.

The terminating officer is (*name and title*)_____.

If there are any problems with or questions about the contents of this fax, call (*name*)

_____, at (*phone*)_____.

Virginia "AMBER Alert" Termination Form for EAS

We are terminating the child abduction alert originated by our agency. Please broadcast the following information.

Text Follows

The Child Abduction Alert which was transmitted earlier for

(*Full name*)_____, abducted from

(*Street*)_____in

(*City or County*)_____, has been

canceled. The Child Abduction Alert for (*Full name*)_____

_____has been canceled.

Text Ends

Originating Agency: _____

Virginia "AMBER Alert" Information Update Form

The enclosed fax is an information update of the Virginia "AMBER Alert" currently activated.

There are (*number*)_____**pages, including this cover sheet.**

The originating agency is (*agency*)_____.

The activating officer is (*name and title*)_____.

If there are any problems with or questions about the contents of this fax, call (*name*) _____, at (*phone*)_____.

Appendix B

VCIN AGENCY ACTIVATION MESSAGE

VCIN AGENCY ACTIVATION MESSAGE

ATTN: ALL VCIN AGENCIES
RE: VIRGINIA "AMBER ALERT"

URGENT URGENT URGENT URGENT URGENT URGENT

THE VIRGINIA MISSING CHILDREN CLEARINGHOUSE HAS JUST ISSUED A VIRGINIA AMBER ALERT IN YOUR AREA. THIS ACTIVATION COULD POSSIBLY INCREASE YOUR 911 CALLS. PLEASE BE ON THE LOOK OUT FOR (CHILD INFORMATION) (WITH SUBJECT INFORMATION if any); (IN A VEHICLE INFORMATION, if any). IF YOU NEED FURTHER INFORMATION PLEASE CONTACT THE (REQUESTING AGENCY/TELEPHONE NUMBER) OR THE VIRGINIA MISSING CHILDREN CLEARINGHOUSE AT (804) 674-2026.

AUTH/Captain Matthew T. Patterson VCIN Control Center/(CNST Name)

VCIN AGENCY CANCELLATION MESSAGE

ATTN: ALL VCIN AGENCIES **(To the same region(s)or statewide, where ever original was sent.)**
RE: VIRGINIA AMBER ALERT

Cancel AMBER Alert **Cancel AMBER Alert** **Cancel AMBER Alert**

THE VIRGINIA MISSING CHILDREN CLEARINGHOUSE HAS CANCELLED THE VIRGINIA AMBER ALERT THAT WAS ISSUED ON (Date) FOR (Child, Suspect and/or Vehicle).

AUTH/ Matthew T. Patterson VCIN Control Center/(CNST Name)

Appendix C

EMERGENCY ALERT SYSTEM (EAS) LOCAL AREAS

EMERGENCY ALERT SYSTEM (EAS) LOCAL AREAS

The Eastern Virginia Local Area

WGH Radio - FM-97.3
5589 Greenwich Road, Suite 200
Virginia Beach, Virginia 23462
757-671-1000

Eastern Virginia Local Area:	Virginia Beach, Hampton, Chesapeake, Poquoson, Portsmouth, Northampton, Suffolk, Accomack, Isle of Wight, York, Newport News, Williamsburg, Norfolk, Surry, James City County, Gloucester, Mathews, Franklin, and Southampton

---

The Richmond Extended Local Area

WRVA Radio - AM-1140
3245 Basie Road
Richmond, Virginia 23228
804-474-0000

The Richmond Extended Local Area:	Greensville, Petersburg, Caroline, Colonial Heights, Emporia, Chesterfield, Sussex Amelia, Richmond, Dinwiddie, Charles City, New Kent, Prince George, Powhatan, Hopewell, Louisa, Hanover, Henrico, King William, King & Queen, Middlesex, Lancaster, Northumberland, Richmond County, Essex, Westmoreland, and Goochland

---

The Fredericksburg Virginia Local Area

WFLS - FM-93.3
10333 Southpoint Landing Blvd, Suite 215
Fredericksburg, Virginia 22407
540-373-9600

The Fredericksburg Virginia Local Area:	Spotsylvania, King George, Fredericksburg, Fauquier, and Stafford

---

The Northern Virginia - D.C. Local Area

WTOP - FM-103.5
5425 Wisconsin Avenue
Chevy Chase, Maryland 20815
202-895-5060

The Northern Virginia - D.C. Local Area:	Manassas Park, Falls Church, Manassas, Fairfax City, Arlington County, Loudoun County, Prince William County, Virginia; District of Columbia, and Prince George's County, Maryland

---

The Culpeper Local Area

WJMA - FM-103.1
207 Spicers Mill Road
Orange, Virginia 22960
540-825-3900

The Culpeper Local Area:	Culpeper, Orange, and Madison

The Charlottesville Local Area

WINA - FM-98.9
1140 Rose Hill Drive
Charlottesville, Virginia 22903
434-220-2300

The Charlottesville Local Area:	Charlottesville, Green, Albemarle, Nelson, and Fluvanna

---

The Farmville Local Area

WFLO - FM-95.7
1582 Cumberland Road
Farmville, Virginia 23901
434-392-4195

The Farmville Local Area:	Buckingham, Cumberland, and Prince Edward

The Southside Local Area

WKJS/WKJM - FM-99.3/105.7
2809 Emerywood Parkway, Suite 300
Richmond, Virginia 23294
804-672-9299

The Southside Local Area: Mecklenburg, Brunswick, Lunenburg, and Nottoway

---

The Danville/South Boston Local Area

WAKG - FM-103.3
710 Grove Street
Danville, Virginia 24541
434-797-4290

The Danville/South Boston Local Area: Charlotte, Danville, Pittsylvania, and Halifax

---

The Roanoke Extended Local Area

WXLK - FM-92.3
3934 Electric Road
Roanoke, Virginia 24018
540-774-9236

The Roanoke Extended Local Area: Henry, Pulaski, Patrick, Giles, Martinsville, Craig, Franklin County, Montgomery, Floyd, Roanoke, Radford, Salem, Botetourt, Bedford, Campbell, Lynchburg, Appomattox, Amherst, Buena Vista, Lexington, Rockbridge, Covington, Allegheny, Clifton Forge, Bath, Highland, Roanoke City, and Bedford City

---

The Shenandoah Valley Local Area

WMRA & WEMC - FM-90.7
983 Reservoir Street
Harrisonburg, Virginia 22801
540-568-6221

The Shenandoah Valley Local Area: Rockingham, Augusta, Page and Shenandoah

---

The Winchester Local Area

WINC - FM-92.5
520 N. Pleasant Valley Road
Winchester, Virginia 22601
540-667-2224

The Winchester Local Area: Warren, Winchester, Clarke, Frederick, and Rappahannock

---

The Marion Local Area

WMEV - FM-93.9
1041 Radio Hill Road
Marion, Virginia 24354
276-783-3151

The Marion Local Area: Carroll, Wythe, Grayson, Smyth, Galax, Bland, and Tazewell

Appendix D

Virginia Missing Endangered Child Alert

Virginia Missing Endangered Child Alert

One of the missions of the State Police and VMCC is to play a central role during the investigation of abducted missing children. One part of that role is assisting the investigating law enforcement agency to publicize the event. The goal is to immediately publicize critical information to other law enforcement agencies, media, and general public in hopes that it can lead to the quick and safe return of the child. To accomplish our mission, there are two categories of notification carried out by the State Police and VMCC: The Virginia AMBER Alert and Endangered Missing Child Media Alert.

The Missing Endangered Child Alert is a viable alternative to the AMBER Alert in those incidents that do not meet all the criteria for an AMBER Alert. Accordingly, when an incident is not authorized for the Virginia AMBER Alert Activation, the requesting agency will be informed that the Department will issue an Endangered Missing Child Media Alert unless circumstances of the incident clearly would not be the intent of either Alert. As a note, the VMCC encourages agencies not to publicize the possible abduction of a missing child as an AMBER Alert until the State Police have indicated that a statewide AMBER Alert will be activated. This recommendation is to ensure that both agencies are aware of the decisions about AMBER Alert activation and there is no disagreement after a local agency indicates an AMBER Alert has been issued.

The Missing Endangered Child Alert uses:

1. Email component notification of the EAS System
2. VMCC, Missing Children website to publish the information
3. Broadcast fax of information to the same AMBER Alert contacts
4. Notification of surrounding states
5. VCIN/NLETS messaging to alert law enforcement agencies
6. Notification of VDOT and posting to their website and employees
7. Notification to the National Center for Missing and Exploited Children
8. Availability of the "A Child is Missing Program"

Once activated, the Endangered Missing Child Media Alert will only send out one broadcast through notification channels. Additional notification will occur if information is updated, to include termination of the Alert. If additional information is received that provides enough detail to qualify as an AMBER Alert, the normal AMBER Alert notification process will occur.

Agencies using the Endangered Missing Child Media Alert will be required to follow the same protocols of the AMBER Alert for submission of information, which can be accomplished by the Law Enforcement AMBER Alert Request website or submission of AMBER Alert forms.

Additionally, agencies will be required to follow other procedures for the investigation, call taking, update of information, and termination protocol. Being familiar with normal Virginia AMBER Alert request procedures will expedite the activation of the Endangered Missing Child Media Alert.

317 DOJ Amber Alert Field Guide for Law Enforcement Officers.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

U.S. Department of Justice
Office of Justice Programs
Office of Juvenile Justice and Delinquency Prevention



AMBER Alert

Field Guide for Law Enforcement Officers

U.S. Department of Justice
Office of Justice Programs
810 Seventh Street NW.
Washington, DC 20531

Caren Harp
Administrator
Office of Juvenile Justice and Delinquency Prevention

Office of Justice Programs
Building Solutions • Supporting Communities • Advancing Justice
ojp.gov

Office of Juvenile Justice and Delinquency Prevention
Enhancing Safety • Ensuring Accountability • Empowering Youth
ojjdp.gov

Unless otherwise noted, photos used in this report are © AMBER Alert Training and Technical Assistance Program.

The Office of Juvenile Justice and Delinquency Prevention is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance; the Bureau of Justice Statistics; the National Institute of Justice; the Office for Victims of Crime; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking.

AMBER Alert

Field Guide for Law Enforcement Officers

May 2019
NCJ 252795

This document was prepared under cooperative agreement number 2017–MC–FX–K003 from the Office of Juvenile Justice and Delinquency Prevention, U.S. Department of Justice.

The opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect those of the U.S. Department of Justice.

TABLE OF CONTENTS

Introduction **1**
Initial On-Scene Response and Investigation **3**
Telecommunications and Patrol First Responders 3
Investigation Response 4
Missing Child Information 5
Suspect Information 6
National Crime Information Center Database (NCIC) Entry 7
Criteria for Adding Persons With Information (PWI) in the Case 8
Establishing Leads/Tips Call Centers and Leads Management **9**
Planning for Call Intake and Leads Management Technologies and Staffing Needs 10
Use of Child Abduction Response Teams (CART) **12**
Search and Canvass Operations **13**
Use of Volunteers **16**
Types of Volunteers 16
Pre-Planning and Management of Volunteers 18
Active Incidents: Coordinating Volunteers 19
The Family's Perspective: Officers' Interaction With Families **21**
Managing Media Inquiries and Coverage **24**
The Importance of Media Training for all Agency Personnel 25
Choosing a Public Information Officer 26
Duties of a Public Information Officer 26
Placement of the Public Information Officer Within the Incident Command System 29
The PIO's Role in the Deactivation Phase of Public Alerting 29
Conclusion **30**

The following individuals are recognized for their contributions to this document.

AMBER Alert Best Practices Working Group

Program Leadership

- James Walters, AMBER Alert Training and Technical Assistance Program (AATTAP)

Project Chair

- Bonnie Ferenbach, AATTAP Digital Experiences Coordinator – Publications, eLearning, and Websites

Representing the National Center for Missing & Exploited Children

- Robert Lowery, Vice President, Missing Children Division
- Alan Nanavaty, Executive Director, Special Programs
- Carly Tapp, Program Specialist, AMBER Alert Operations

Representing AATTAP Region 5

- Carri Gordon, Washington State AMBER Alert Coordinator and Program Manager, Washington State Patrol Missing and Unidentified Persons Unit | AATTAP Associate and Region 5 Liaison

Representing AATTAP Region 4

- Chuck Fleeger, Assistant Chief of Police, College Station, Texas, Police Department | AATTAP Associate
- William Smith, Special Agent in Charge, Kansas Bureau of Investigation | Kansas AMBER Alert Coordinator and Program Manager

Representing AATTAP Region 3

- Michelle DuBois, Program Coordinator, AMBER Alert Program and Wisconsin Clearinghouse for Missing Persons, Wisconsin Department of Justice, Division of Criminal Investigation

Representing AATTAP Region 2

- Gus Paidousis, AATTAP Associate and Region 2 Liaison



I Introduction

Reports of endangered missing and abducted children may be among the most difficult, challenging, and emotionally charged cases that law enforcement first responders and investigators will ever experience. Each stage of the case, from the initial call through recovery, forms a critical component of a thorough child recovery response. Public safety agencies must provide their staff with the tools and training that enable them to act swiftly and decisively when confronted with these types of cases. An immediate and comprehensive response enhances the likelihood of accumulating evidence or information that might otherwise be lost during the critical, early stages of an investigation.

As first responders in a missing child investigation, local law enforcement plays a critical role in the overall life cycle of the investigation and the use of the AMBER Alert public notification system, if warranted.

The AMBER Alert system is useful only when agencies know how and when to activate an alert. Agency policies and procedures should clearly outline the investigative response to a missing child, to include the procedures and lines of authority for requesting an AMBER Alert. Law enforcement's investigative processes are inherently separate and different from the AMBER Alert process in a child abduction case. They may involve different agencies, personnel, and timing; however, they are still inextricably connected and interdependent if an AMBER Alert is ultimately issued. An effective initial response by law enforcement feeds the core information to the authorities who can issue an AMBER Alert. A successful alert, in turn, will trigger a significant influx of tips and leads in the case.

This guide is designed to help law enforcement better understand how to avoid or mitigate critical pitfalls in a child abduction case. These can include delays in requesting an AMBER Alert due to officers not knowing whom to call and what core information to provide for an effective alert. It is also critical for law enforcement officers to know that it is okay to call the AMBER Alert Coordinator early in the case to discuss options for the alert, even as information is coming together in the investigation.

The following information was developed by subject matter experts who have been active in AMBER Alert programs throughout the country. It includes the following suggested practices for some key areas of the law enforcement response:

- Initial on-scene response and investigation (patrol, supervisory officers, and investigators);
- Establishment of lead/tip call centers and management of lead/tip information;
- Use of Child Abduction Response Teams (CART);
- Deployment of search and recovery operations;
- Use of volunteers;
- Officers' interactions with family members; and
- The role and responsibilities of a Public Information Officer (PIO).



AMBER ALERT ISSUANCE CRITERIA AND STATE AMBER ALERT PROGRAM CONTACT INFORMATION

U.S. Department of Justice-recommended guidelines for issuance of an AMBER Alert can be found on the AMBER Alert and on The AMBER Advocate websites.

For an interactive map of state AMBER Alert program contact information, visit the Meet our Partners page on The AMBER Advocate website.

Another 24/7 resource for AMBER Alert assistance is the National Center for Missing and Exploited Children: 1-800-THE-LOST.



1 Initial On-Scene Response and Investigation

Telecommunications and Patrol First Responders

The investigation begins when the call is received by the telecommunicator, who works carefully through a pre-defined intake protocol to gather key information about the location and nature of the emergency, along with identifying information on the child, suspect (if known), and vehicle (if known). Based on call intake, the telecommunicator allocates appropriate resources and works with patrol officers to ensure a rapid on-scene response. The telecommunicator continues to be part of the initial response by taking in additional information via phone and radio transmissions, documenting all information for later retrieval and analysis. Patrol officers should proceed directly to the scene, secure appropriate locations, identify and interview family members and witnesses, establish perimeters, and work to verify and build on the information gathered during initial call intake. Additional tasks can include preliminary search and canvass efforts, if appropriate. All of these actions support swift, thorough, and accurate information gathering for the creation of a missing person entry and associated records on the suspect and vehicle involved. By federal mandate, this information is entered into the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC) within two hours of the first report of the missing child. Activation of an AMBER Alert should be considered at the earliest stages of the response, and appropriate authority should be given to field personnel when the need for these resources is identified.

©Rosemary Ketchum/Pexels.com

Investigation Response

For investigators, the response conducted cooperatively by telecommunications and patrol forms a foundation from which to effectively move the case forward – with canvass, search, interviews, and forensics – as all parties work rapidly and strategically to locate and safely recover the missing child. The information gathered during the preliminary investigation is supplemented through continued efforts and can lead to a request for an AMBER Alert at any point in this process. If it is determined that the case will be better handled through other methods available to the department, such as an Endangered Missing Advisory (EMA), the AMBER Alert Coordinator will advise on the alternative and direct that process as well. See *Guide for Implementing or Enhancing an Endangered Missing Advisory* for more information.

To activate an AMBER Alert, the AMBER Alert Coordinator must be confident that an abduction has occurred, the criteria for activation have been met, and the local agency has ruled out any other possibilities for the child's disappearance. Because every minute matters in such situations, as much information as possible must be collected in the early stages of the investigation and carefully assessed to drive the best decision about alerting the public in the case. It is important to remember that the AMBER Alert is just one tool, albeit an important and powerful one when warranted, that can be utilized when a child is abducted. Other investigative and search techniques must also be used rapidly and effectively in the initial stages of the investigation.



PATROL AND INVESTIGATIVE FIELD RESPONSE CHECKLISTS

Detailed response checklists for patrol officers, supervisors, and investigators are available for download on the AMBER Alert Best Practices resource collection page on The AMBER Advocate website.

Missing Child Information

During the initial call intake, patrol officers' first response, and preliminary field investigation, law enforcement is working to obtain, verify, and build out the following information about the missing child.

Primary Identifiers

Primary identifiers are those most recognizable for visual identification by officers and the public, and those that are immediately needed for the telecommunicator to begin NCIC entry:

- Name, including nicknames;
- Date of birth;
- Race;
- Gender;
- Physical description (height, weight, hair color, eye color, scars/marks/tattoos, clothing last seen wearing);
- Physical anomalies or recognizable physical attributes such as a limp, tick, or physical behavior;
- Notable items the child may be carrying, such as a backpack, purse, or comfort item such as a special blanket, doll, or stuffed animal; and
- Current and realistic photographs, digital images, and videos of the child as he/she looks every day.

Caution/Medical Information

Advisories urging caution and to provide medical information are critical for notifying first responders and other law enforcement officers about any medical conditions the child may have or immediate threats to the child's physical safety, such as known or suspected weapons:

- Blood type, if known;
- Medical conditions (such as diabetes, asthma, epilepsy);
- Neurological/behavioral conditions (autism, attention deficit hyperactivity disorder, attention deficit disorder);
- Medications the missing child is taking or needs to take (name, type, such as pill, injection, or inhaler) and time last taken, if known; and
- Known or suspected weapons involved with the child's disappearance or abduction.

Additional Information

The following information is important for packing the NCIC record and getting basic incident, victim, and suspect information to investigators – and to support alerting the public:

- Social Security number;
- The child's cell phone number, and description/location of any other computer or mobile devices the child has or uses;
- Email address(es);
- Facebook, Twitter, Instagram, Snapchat, or other social media accounts/ screen names; also ask about any online gaming platforms/sites the child uses;
- Reasons why the reporting person believes the child is missing;
- The child's normal routines and any past history of running away;
- Any circumstances that may indicate the disappearance was not voluntary and the child may be in imminent danger;
- Name and location of the child's school;
- Name and location of the child's dentist and primary care physician, if known; and
- Name and location/address of any friends the child could be with or could have spoken to at/around the time of the disappearance or abduction.

Suspect Information

Law enforcement should work from initial call intake through the field investigation to obtain, verify, and build out the following information about the abductor, if known:

- Name, including any aliases or nicknames;
- Relationship to the missing child (e.g., family member, friend/associate, acquaintance, stranger to the child);
- Race;
- Gender;
- Physical description (height, weight, hair color, eye color, scars/marks/ tattoos, clothing last seen wearing);
- Physical anomalies or other recognizable physical attributes;
- Date of birth;
- Vehicle information if one is known or suspected to be used in the crime: color, year, make, model, body (rust, dents, stickers), license/tag, state of tag;

- Any known or suspected weapons used/in possession of the suspect;
- Criminal history;
- Companions or associates the suspect may be with or going to see;
- Possible direction of or routes of travel – including any public transit the suspect may be likely to use;
- Places the suspect may be going;
- Cell phone number;
- Email address(es);
- Facebook, Twitter, Instagram, Snapchat, or other social media accounts/ screen names; and
- Any online gaming platforms/sites the suspect is known to use or suspected of using.

National Crime Information Center Database (NCIC) Entry

As soon as it has been determined that the child is missing and sufficient information is obtained, the agency should enter the information into the NCIC database. Section 104 of the Adam Walsh Child Protection and Safety Act of 2006 amended the reporting requirement set forth in Section 3702 of the Crime Control Act of 1990 (42 U.S.C. 5780) by changing "immediately" to "within two (2) hours of receipt." The FBI guidelines further define the entry criteria as "two (2) hours after enough information has been obtained to enable the entry into NCIC."

The appropriate flag should be set to indicate either Child Abduction (CA) or AMBER Alert (AA). The entry should include as much information as the responding officer can provide, including realistic/current **images of the child**. The **miscellaneous field should be used for all pertinent details** of the case for which there are no defined entry fields.

The investigator should work with telecommunications staff to ensure regular review and update/modification of the NCIC record as new information is gathered in the case through interviews, canvassing, and searches. This includes cancellation of the NCIC record when the child has been safely recovered. The record should be canceled only after full confirmation that the missing child has been found is received from law enforcement personnel.

Criteria for Adding Persons With Information (PWI) in the Case

NCIC provides a searchable Persons With Information (PWI) field where the details of a person who may have information about the child, or who is possibly connected to the missing child, can be added and linked to the child's record when a warrant has not been issued. The person must have been identified to the public, either through an AMBER Alert or other notification; must be believed to have relevant information that could aid in locating the child; and cannot be located, with time being of the essence. For questions about entering and managing missing person records in NCIC, review the resource *Effective Use of the National Crime Information Center Database With Missing Child Incidents.* To obtain the FBI's *Data Collection Entry Guide for Missing Persons,* or for more information on PWI or other NCIC functions, contact NCIC at 304-625-3000.



2 Establishing Leads/Tips Call Centers and Leads Management

Once an AMBER Alert has been issued, the influx of information to the investigating agency will increase exponentially. The success of the ongoing investigation depends on the ability of law enforcement agencies to receive, process, and prioritize leads and tips without dropping calls or otherwise missing incoming leads received by text message, social media, or field report. Coordination of this critical function is vital to the successful recovery of a missing child and possible prosecution of the offender(s). Many times, lack of prior planning may force an agency to direct calls into its existing law enforcement communications center via 9-1-1 or other published emergency lines. Depending on the number of operational consoles and phone lines, and how these are staffed, this can bottleneck an agency's capacity to process normal calls for service while attempting to take in tips, disseminate them, and properly manage records for investigative leads in the case.

A series of activities should be performed to ensure the effective operation of a tips and leads management system. These activities include:

- Securing equipment and establishing use agreements (if shared between agencies) for regional phone and/or computer banks;
- Identifying, procuring, and performing testing and technical training on call-stacking/rollover systems, electronic leads capture, dissemination, and tracking;
- Establishing a plan that outlines all phone and text numbers available and authorized for use by the public, as well as any unpublished numbers to be used by law enforcement and other authorized partners in the case;

©Pixabay/Pexels.com

- Creating call-out notification and staffing plans;
- Developing plans and procedures for intake of calls and texts, including detailed training for all staff; and
- Establishing contingency procedures for outside agency support in those cases that become long-term or otherwise require multi-agency and/or jurisdictional response.



CALL INTAKE AND LEADS MANAGEMENT OPERATIONS PLANNING

Consider establishing an agreement with the Emergency Operations/ Fusion Center, if one is available in your area, for use of their joint communications area during an AMBER Alert activation. This allows leveraging of existing infrastructure to accommodate the volume of calls that may be received with an active AMBER Alert.

For resources in this area, visit the AMBER Alert Best Practices resource collection page on The AMBER Advocate website.

Planning for Call Intake and Leads Management Technologies and Staffing Needs

Rapid and coordinated sharing of case information between all area law enforcement communication centers will help to mitigate the problem of failing to route all calls relating to the child abduction to the agency overseeing the investigation. Appropriate venues that could be utilized for such an incident should be researched prior to the emergency to avoid having to route case-related calls through an active dispatch center that will still have to maintain day-to-day operations. The designated call center should have caller ID, phone line recording to capture all conversations, as well as stacking and rollover capabilities. These functionalities will help to ensure that all calls are answered as swiftly as possible, that pertinent data and records can be verified, and that calls are not lost.

Child abduction incidents can become overwhelming in the amount of information generated by the activation of an AMBER Alert and subsequent community involvement. Managing that information as part of the investigation leaves no room for error in the intake, storage, analysis, and retrieval of data coming from a multitude of sources. Proper planning, research, and selection of a designated leads management system should be undertaken before any incident that might involve its deployment and use. Ongoing training should develop and maintain staff proficiency in that designated system, and periodic testing will help to ensure that both the staff and the system will be ready at the needed time. Methods for obtaining additional resources, including resource sharing and vendor assistance, should be explored to support enhancements to the call intake and leads management system.

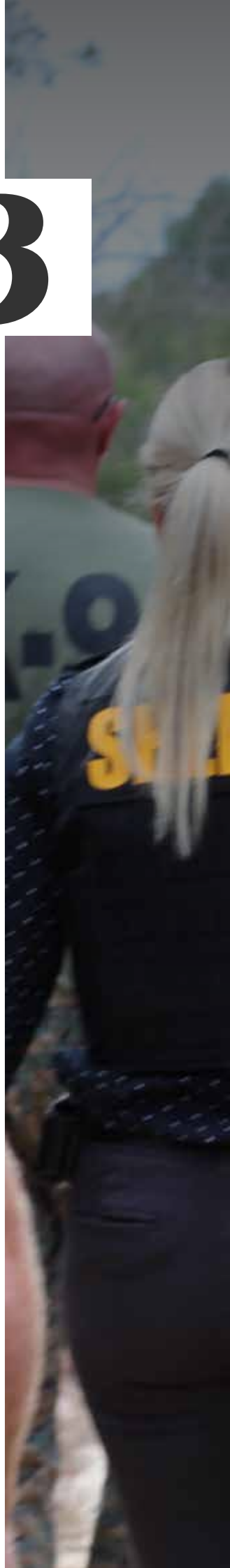
Proper staffing and supervision structures must be in place to ensure effective oversight, operation, and monitoring of the tips intake and leads management system implemented for your agency and/or jurisdiction (if a multi-agency partnership). Workstations should be staffed by specially trained personnel who have scripted questions and functional working knowledge of the leads tracking or case management system in place. Documented workflow procedures that guarantee all information is evaluated, routed, followed up on, and documented in a consistent manner will ensure a proper response to every call taken and lead developed. Although volunteers are sometimes used for this operation, doing so is not recommended. Best practices include using experienced call-takers/ telecommunicators and sworn officers, who are better prepared to perform thorough intake, prioritization, investigation, and management of leads.



©Andrea Sutherland/Flickr.com

Use of Child Abduction Response Teams (CART)

3



Like an AMBER Alert, a Child Abduction Response Team (CART) is a resource that law enforcement agencies can employ in an abduction incident or in situations where a child is missing and believed to be in danger. While activation of a CART may occur in a case, it should never supersede the handling agency's immediate and initial response and investigative work.

A CART is a multi-agency, often multi-jurisdictional team of professionals who are trained and equipped to respond in the search and recovery of an endangered missing or abducted child. The CART strategy incorporates three elements: trained individuals with established roles and assignments, a readymade list of equipment available to aid in the search, and a network of multi-disciplinary resources the team can utilize in the investigation. If an agency participates in or has access to a CART, it should consider requesting the team's activation very early in the investigation to assist in the multitude of tasks that will need to be accomplished, such as conducting a neighborhood canvass, accounting for sex offenders in the area, and following up on leads generated by public alerting. Much like SWAT, CART provides assistance and support for these low frequency but extremely high criticality responses. More than 300 active CARTs representing 48 states, the District of Columbia, Puerto Rico, the Bahamas, and Canada have received training through the Office of Juvenile Justice and Delinquency Prevention's AMBER Alert Training and Technical Assistance Program. For more information about CART training or establishing a CART program, visit The AMBER Advocate website's CART Resource collection.



4 Search and Canvass Operations

Many law enforcement agencies do not have an established plan or procedures for conducting canvassing or a search as part of a missing child investigation. As with any skill set, these abilities can erode over time if not practiced regularly. While the CART should bring in highly trained team members to build on early efforts, it is very important that all agencies have the knowledge and skills to effectively begin this process and establish an effective foundation for subsequent investigative efforts. A historical analysis of canvass and search operations reveals a number of serious problems that have occurred during major investigations:

- Missed witnesses;
- Missed, damaged, or destroyed physical evidence;
- Failure to identify and document all parties residing/ present in homes and businesses canvassed;
- Poor documentation of interviews, places that have been searched/canvassed, crime scenes, and other investigative work conducted;
- Poor coordination and centralization of documentation/ records and updates as field personnel work the case, resulting in confusion, duplication of efforts, and/or missed leads;
- Officers being unaware that they have had contact with suspects;
- Delays in initiating formal search activities;
- Difficulty in obtaining feedback from those performing canvass operations;
- Ambiguous chain of command or lines of authority for operations;

- Inadequate use of specialized resources available in the area;
- Poor interagency communications, both from a lack of contact information and from technical/interoperability issues;
- Lack of preparedness for managing unanticipated volunteer response; and
- Unplanned and/or poorly managed work with the media to protect the integrity of information and provide regular updates in the case.

The importance of conducting a thorough, organized neighborhood canvass using only trained professionals (and, whenever possible, sworn law enforcement officers) with scripted questions cannot be overstated. These trained resources should be dedicated in their assignment and not subject to being called away or reassigned until after the canvass of the assigned area is completed. The information gained through these canvass efforts must be analyzed as part of the lead management process to ensure that all persons and locations within a designated area are covered prior to deeming that area "complete."

Canvass operations are manpower-intensive endeavors that will take a significant amount of time to perform correctly. The procedures listed below are based on the findings of the Case Management for Missing Children Homicide Investigation Study, conducted by the Washington State Attorney General and the Office of Juvenile Justice and Delinquency Prevention. Practitioners recommend that investigations personnel complete these actions as part of their canvass operations.

- **Repeat the neighborhood canvass the day following the abduction,** beginning with areas where the suspect may have been 30 minutes before the actual time of the abduction. The study found that killers were in the area of initial contact in 67 percent of the cases studied – often living in the area or engaging in normal activity, such as employment or other routine business. Additional canvass efforts should be repeated as needed on the same day of the week and same day of the month as the abduction to reach as many persons with information as possible.
- **Look at the area from different vantage points;** obtain and study current aerial pictures and/or current satellite imagery, if possible. Researchers found that the victim's last known location was usually very close to the site of the initial contact between the killer and the victim. When police did not know the killer's initial contact site, case solvability dropped to just 24 percent, as opposed to nearly 80 percent when police had information about the initial contact site.

- **Pay close attention to individuals who have recently moved into or out of the area.** The study revealed that after the crime was committed, 16 percent of murderers left town and 10 percent interjected themselves into the murder investigation, usually during the search operation.
- **Check all registered sex offenders in the area and verify this information** against any database that contains information about these individuals. The local agency can utilize its state sex offender registry, the National Sex Offender Registry, and can contact the National Center for Missing & Exploited Children (NCMEC) 24/7 at 1-800-843-5678 for support in this critical area of the investigation. Keep in mind that there are a large number of non-compliant sex offenders across the country, and these individuals will be singled out in an ongoing investigation only by identifying all persons associated with a certain area during canvass operations.
- **Gather information about cellular and internet-connected devices.** Agencies should utilize local, state, or federal subject matter experts to obtain data from cellular and internet service providers that are critical in determining a suspect's and/or a victim's activity, including possible location or routes of travel. This can help to corroborate witness statements regarding the missing child and/or suspect. If resources are not available at the local or state level, the U.S. Marshal's Service can assist agencies with this work. Additionally, the Internet Crimes Against Children (ICAC) Task Force in operation within the state can assist with this work.

5 Use of Volunteers



Volunteers can be an asset in the search and recovery of a missing child. However, if not properly screened, trained, and prepared, they can compromise the operation. An agency-assigned volunteer coordinator should create a plan that specifies how volunteers will be used as a resource in missing child cases.

Types of Volunteers

Agencies can incorporate a volunteer protocol within their plan in one of two ways. Best practice emphasizes proactive planning for use of volunteers by identifying and establishing procedures for call-out of volunteer groups that are pre-selected and trained for use with missing child incidents. Such groups include local search and rescue teams, citizen police academy graduates, and auxiliary police officers as well as Community Emergency Response Teams (CERT) already established in many communities across the country. Other agencies maintain an ongoing volunteer recruitment program to identify and prepare members for use in various agency operations.

If an agency does not have the ability to utilize a predetermined volunteer contingent, at minimum they should specify clear policy and procedures for requesting, selecting, and screening volunteers on a case-by-case basis. Policy should also detail the types of assignments for which volunteers may be used. Being prepared to address spontaneous volunteers who will arrive onsite during active incidents to offer their services is critical. Without a plan for vetting and training spontaneous volunteers, including an orientation process, these volunteers are very

VOLUNTEER RESOURCES

Agencies may identify and proactively establish agreements with local, regional, state, or national groups to provide pre-vetted and trained personnel assistance with leads/tips management and field support, such as search and rescue functions. Examples would include:

- The National Center for Missing & Exploited Children
  - » Project ALERT (forensics and biometrics support for law enforcement);
  - » Team HOPE (surviving families who support one another during and after cases);
  - » Team Adam (on-scene support to law enforcement and families);
- Emergency response teams;
- Search and rescue teams;
- Explorers, recruits, and military reserve units;
- Citizen police academy participants and alumni; and
- National Guard units.

The U.S. military is authorized to assist local jurisdictions in the event of a missing child. Contact the Air Force Rescue Coordination Center Console Operations at 850-283-5955.

likely to create extra work for law enforcement officers who are forced to direct volunteers rather than focus on their primary job, which can negatively impact investigative response. Although both established volunteer groups and individual ad-hoc volunteers can offer skills and resources before, during, and after an emergency, agencies must ensure they are prepared to utilize them effectively and appropriately during active cases.

Pre-Planning and Management of Volunteers

As previously emphasized, departments should do everything possible to have a pre-established team of volunteers to allow time for vetting, background checks, and management of records related to the volunteers involved. When spontaneous volunteer contingents are used, many of these critically important functions are not feasible due to time constraints and other logistics, and their omission can potentially jeopardize the investigation.

Management of volunteers should include the following actions:

- Conduct background checks on volunteers or use volunteers who have already been cleared by background checks;
- Ensure volunteers have correctly completed registration and waiver of liability forms;
- Photograph all volunteers and include them on identification badges distributed during active use/events (if photos are not possible, at minimum include the volunteer's full name);
- Maintain a volunteer log with name, photo, date of birth, phone, address, email, skills/expertise relative to their role, and all other agency-mandated information; update this information at least quarterly; and
- Hold periodic training sessions, to include:
  - » Current issues, legal updates, and investigative findings having implications for their work in assisting with endangered missing and abducted child cases;
  - » Protocols to be followed during the search, including personal/team safety, areas authorized for search, and reporting actions for witnessed events or locating evidence; and
  - » Mock activation/call-out exercises and training debriefs.

Volunteer management resources, such as sample applications and other forms/ templates, are available for download in the CART Resource collection on The AMBER Advocate website.

Active Incidents: Coordinating Volunteers

During active incidents, the volunteer coordinator should take the following actions:

- Brief volunteers properly prior to deployment as to assignment and expectations;
- Ensure that volunteers are closely supervised throughout the duration of the incident (consider assigning a law enforcement officer or a trained/vetted volunteer supervisor to each search group);
- Instruct volunteers not to talk to the media – all announcements and updates will come only from the designated media representative;
- Instruct volunteers to be mindful of evidence they may encounter and to not remove or touch any items they may find;
- Remind volunteers that they cannot discuss case-related activities with family or friends;
- Maintain control over the search, volunteers, public safety personnel, and others on the scene; and
- Check with volunteers periodically for signs of stress or fatigue (rotate volunteers as needed to ensure their safety and effective execution of duties).

Ensure that food and drink, along with necessary equipment, are provided during the search. When the search has concluded, the coordinator should take the following actions:

- Provide a comprehensive debriefing for volunteers to include any officers or other employed personnel who were assigned to volunteer operations. Discuss what went well and what should be done differently with future incidents to promote increased safety and effective response.
- Give volunteers as much information about the case as the investigation will allow, while emphasizing the confidential nature of information concerning the case and clearly noting the reasoning for any information that cannot be disclosed at this juncture.
- Thank volunteers for helping with the search. If possible, send letters of appreciation within two weeks of the event. Taking care of volunteers and expressing thanks is the best way to promote participation in future searches.

Post-Incident: Volunteer After-Care

The work of search and rescue volunteers in endangered missing and abducted child cases can be both physically and emotionally taxing, with long-lasting impacts that may need support to resolve. If volunteers are not already part of a professional search organization that provides after-care such as debriefs, counseling, and grief support, it is important for law enforcement to identify local resource providers to whom volunteers can be referred if needed.







6 The Family's Perspective: Officers' Interaction With Families

The Office of Juvenile Justice and Delinquency Prevention and the AMBER Alert Training and Technical Assistance Program convene an annual roundtable event during which family members and survivors of missing and abducted children come together to share their experiences and to help law enforcement better understand how enduring the disappearance or abduction of a child or sibling affects them. In the face of the anxiety, fear, and horror that comes with these incidents, law enforcement's approach to working with the family during initial response, public alerting, ongoing investigation, and court prosecution proceedings has profound and lifelong impacts on the family – and the victim if safely recovered.

OFFICE OF JUVENILE JUSTICE AND DELINQUENCY PREVENTION – AMBER ALERT TRAINING AND TECHNICAL ASSISTANCE PROGRAM FAMILY ROUNDTABLE EVENTS

AMBER Alert Coordinators and other AMBER Alert Partners can read past Family Roundtable Reports by logging into The AMBER Advocate website's Partners Portal and visiting the Partner Resources area.

Resources for families can be found at The AMBER Advocate website's Community Resources area.

The National Center for Missing & Exploited Children's website has a Victims and Family Support page and a Publications page.



©Anastasiya Lobanovskaya/Pexels.com

Invaluable insights and recommendations on what law enforcement did well, and what they could have done better, have been gained from these roundtable events.

- Family advocates should be identified by law enforcement agencies, and call-out/response agreements established to ensure that an advocate can be assigned to the family as early in the case as possible. Family advocates provide a critically important liaison between the investigative operations and the needs of the family, helping in the following ways:
  - » Communicating information and updates;
  - » Ensuring the family understands what is happening in the case and why;
  - » Assisting the family in dealing with media inquiries;
  - » Supporting the family during the recovery and/or reunification phase of the case; and
  - » Supporting the family through prosecutorial developments and court appearances as the case is adjudicated.
- In-service training on policies and procedures to be followed with missing children cases should be mandated for first responders, including telecommunicators and patrol officers, with retraining at least once every two years:
  - » First responders and investigative officers should be trained on how to interview and communicate with parents and other family members in a way that allows them to gather information while being sensitive to what the family members are going through; and
  - » Crime scene professionals should be trained on the importance of evidence collection and preservation in missing children cases.
- Every first responder should utilize protocols and checklists when working a case to ensure that critical actions are not inadvertently omitted during the chaos often associated with these types of events.
- Law enforcement agencies should have the capability to rapidly deploy canvassing as well as search and rescue resources (such as K-9 tracking, underwater search/rescue, and geo-tracking/mapping) in endangered missing and abducted child cases.
- Officers should act immediately and treat the case as an endangered missing child case unless and until significant facts are confirmed otherwise.

- Officers should ask the parents for recent photos or digital images (including video) that depict the missing child as he or she looks now/realistically.
- Officers should treat the home as a crime scene but attempt to leave the home in the condition in which they found it.
- Officers should give parents the details, even the hard ones, before they give information to the media.
- Officers should never assume the child is a runaway or make statements such as "They will probably come home in a few days." If the missing child is an adolescent or teenager, law enforcement should not stereotype him or her as a runaway. This assumption can hinder the immediate implementation of comprehensive recovery actions. It is important for law enforcement to proceed based on what the parents are saying and verify the information accordingly.
- Law enforcement should understand compliant behavior and the dynamics of abduction-luring, also known as "learned helplessness," so as not to make assumptions or draw incorrect conclusions when investigating cases where a child willingly left or stayed with the abductor, even if the child may have had opportunities to escape.
- The family's socioeconomic status should have no bearing on how law enforcement handles a case.



Managing Media Inquiries and Coverage

7

Keeping the child's image in the mind of the public is key to the investigation. The intense media coverage during an AMBER Alert often supports recovery of the child and in some cases has resulted in the abductor releasing the child to avoid apprehension.

No law enforcement agency should be without a Public Information Officer (PIO) during these critical incidents. The PIO's presence will be particularly prominent during the early stages of a case when press conferences, media interviews, and similar events will keep his/her name and face, but more importantly the child's name and face, in the public eye. The PIO establishes the overall tone with the media and public, and works to manage the flow of information based on legal restrictions and agency policies.

Ideally, the PIO should be involved from the very beginning of incident command to ensure that the appropriate information is released to the media and to avoid any misinformation being an issue with the media. The best way to ensure the PIO is included in all aspects of the incident's progression in terms of media updates and public reporting is to define the PIO's responsibilities clearly in the law enforcement agency's missing child policies and procedures, to include special considerations for cases in which public alerting (AMBER Alert or an Endangered Missing Advisory) is utilized.

A law enforcement chief executive officer (CEO) once commented that "activating an AMBER Alert is like sending up a flare asking every media outlet to critique the way you are handling



©Pixabay/Pexels.com

your investigation." The PIO role, when executed effectively, helps to mitigate misinformation and unfounded criticism by facilitating the media's accurate coverage of when and why an AMBER Alert or other public alerting tool was activated, along with providing precise information that enables the public to look out for and report useful tips or leads to law enforcement.

The Importance of Media Training for All Agency Personnel

While it is important to designate a specific face and message for the incident in the form of a consistent PIO, every member of all the agencies involved needs to be aware of his/her role in information security. With the proliferation of news outlets and the need to remain ahead of their competitors in the 24 hour news cycle, the tactics of members of the media have become increasingly aggressive and multi-faceted. While reporters and journalists will continue to seek out information through traditional means, such as news releases and press briefings, they will also actively seek out and solicit news sources close to the investigation. This has been seen with documented cases of media outlets monitoring scanner traffic as well as conducting surveillance on agency parking lots and following vehicles they believe to be heading to locations of interest. Employees of agencies involved in the case, whether sworn or civilian, must know that they could inadvertently become an unintentional "source close to the investigation" if approached by media representatives.

The PIO's primary function during an endangered missing or abducted child investigation is to convey accurate and timely information from the law enforcement agency handling the case to the public via traditional media outlets, as well as website and social media accounts managed by the agency, to keep the child's image and the story in the news. Through planning and regular communication, the PIO also works to build and maintain an effective partnership between the media and law enforcement in working to promote swift location and safe recovery of missing children.

Choosing a Public Information Officer

Ideally, the PIO should be employed full time for the law enforcement agency and have a strong functional knowledge of policy and procedures for the agency's release of information to the public via the media. While larger agencies usually have a full-time PIO on staff, smaller departments often lack the personnel or resources to employ a dedicated PIO. In this case, they may assign the responsibility on an as-needed basis to another officer, or rely on other agencies within their jurisdiction or the state police to provide this service. Regardless of the approach to fulfilling this important role, any officer designated as a PIO should then be trained and prepared to work effectively with the media and the public when incidents occur.

The law enforcement agency's CEO must have confidence in the PIO, and the PIO must be able to function within the CEO's authority. While the PIO's public-facing role is to partner with the media to provide the public with information about the case, the PIO must maintain the focus on the primary goal, which is to protect the investigation and law enforcement's ability to safely recover the missing child. To do this effectively, the PIO must have fluid access to information, key agency personnel (including the chief or sheriff), the crime scene area, and other areas where information may be generated.

Duties of a Public Information Officer

Core Areas of Work

The PIO works to accomplish these essential, overarching functions:

- Notifies the public through all available resources to be on the lookout for the missing child;
- Enhances media coverage of the missing child incident by providing photographs, videos, and other visual aids to help identify the victim(s) and/or suspect(s) and the vehicle(s) used in the abduction;
- Helps oversee and coordinate all social media campaigns to recover the missing child;
- Ensures the story stays alive by providing regular updates with accurate and timely information appropriate for sharing with the public;

- Gauges public opinions and media perceptions for the investigating agency, addressing any issues and ensuring the focus stays on the child;
- Anticipates possible worst-case scenarios and prepares the agency's response to the types of questions likely to accompany such scenarios; and
- Provides family members and others involved with effective strategies for conducting media interviews and press conferences – with a focus on their privacy, dignity, and well-being – while also safeguarding the investigatory details of the case.

Organizing Media Briefings

The PIO should be responsible for all logistics involving media briefings, including creating the briefing schedule, establishing the location of the briefings (away from the command center if possible), and securing parking and staging areas for media vehicles.

When conducting media briefings, the PIO should take the following actions:

- Choose a location for the briefing area that will meet the needs of both investigators and the media. Consider parking lots and other public areas rather than law enforcement headquarters;
- Plan for a worst-case scenario by anticipating all types of questions likely to arise in such a scenario and the agency's response;
- Work with family members to prepare them if they are to be a part of the briefing. Use a victim advocate to assist and prepare the family;
- Work with media technicians to supply image, audio, and video content (approved by incident command) to be broadcast as part of media briefings and newscast updates;
- Set the tone for the media briefing. Maintain control of the entire briefing environment (e.g., where it takes place, participants' roles, and structure of the briefing);
- Start every media briefing with an opening statement by an appropriate law enforcement official followed by a question-and-answer dialog (if previously agreed to by law enforcement officials); and
- Provide all appropriate information – in addition to photos and video footage – on the victim, suspect, vehicle, and possibly crime scene or location insofar as it will enhance the public's ability to assist the law enforcement investigation.

Responding to False or Unfounded Information

Rumors and false or misleading information frequently emerge during any law enforcement incident or investigation; endangered missing and abducted child cases are no exception. Because journalists will seek additional information on their own from a victim's family members, friends, and witnesses, rumors can develop quickly. It is important for the PIO to monitor rumors and stay informed about all aspects of the investigation. The PIO is responsible for doing everything possible to ensure that the information delivered to the public is accurate and timely in an effort to mitigate potential problems as the case progresses. The PIO should take the following actions:

- Monitor all media coverage of the incident, including broadcast news, radio, websites, and social media;
- Collect as much information as possible about any rumors that are circulating, correcting information through media updates and postings to agency web pages and social media platforms;
- Contact the appropriate media outlet(s) directly to address incorrect information and supply corrections to be conveyed to the public;
- Recognize that the media are participating voluntarily and do not want to be viewed as an extension of law enforcement. The media respect law enforcement agencies much more when they recognize that the media's primary responsibility is to inform the public independently;
- Be aware that once an AMBER Alert has been activated, the story will be pursued aggressively. This means the angle of the story may change in unpredictable ways. The AMBER Alert process may be analyzed and the criminal investigation scrutinized – all in the public domain, with little or no direction from law enforcement; and
- Be aware that some information the media uncovers may need to be investigated. In most cases, the media will provide a copy of broadcast and/or written materials on request, so make that request before pursuing a court order for seizing the materials.

Placement of the Public Information Officer Within the Incident Command System

The Incident Command System represents a component of the Federal Emergency Management Agency's National Incident Management System protocol as required by U.S. Department of Homeland Security statutory regulations. The PIO should be strategically placed within the agency or jurisdictional Incident Command System to allow him/her to report directly to the incident commander and communicate with all law enforcement personnel in command of the various investigative components of the operation. Access to information is essential for the PIO to establish a smooth flow of information to the public and to monitor how well the media are disseminating details about the incident. A PIO who is involved in the agency's key decision-making processes is positioned to ensure that the media receive only messages that will responsibly inform the public about the agency's search for a missing child.

The PIO's Role in the Deactivation Phase of Public Alerting

When an AMBER Alert is utilized, the alert should be deactivated when the child is recovered, even if the suspect is still at large. The deactivation of an AMBER Alert will likely require the PIO to initiate the following actions:

- Inform victims' families about the most effective ways to deal with media attention and the pros and cons of being interviewed by the media. In addition, the PIO should advise families about information they should and should not discuss, in accordance with the advice of investigators and prosecutors working on the case;
- Work with the prosecuting attorney to ensure that the release of information will not jeopardize the ability to obtain a conviction in the case if the subject was arrested, or if the subject is later located and charged; and
- Acknowledge, on behalf of the agency and its CEO, the contributions of everyone involved – television and radio broadcasters, news organizations, cellular and internet service providers, local businesses, volunteers, government agencies, and law enforcement agencies that supported the effort with coverage, volunteer services, staffing/personnel, and other resources.

Conclusion



The work and processes that first responders and investigators undertake when a child is reported missing or abducted are of primary importance for law enforcement in the effective planning, training, and operational response to these critical incidents. The focus of the AMBER Alert Program is to increase the likelihood of safe recovery through immediate public awareness and identification efforts in endangered missing or abducted child cases where public notification can be of benefit to the investigation.

The AMBER Alert process is designed to support existing law enforcement protocols that are initiated as part of the established investigative response to endangered missing and abducted child incidents. The anticipation of, or decision to issue, an AMBER Alert does not replace, rescind, or supersede the work of normal first responder and investigative functions when a child is missing.

The process of gathering the required information and approvals toward the activation of an AMBER Alert may necessitate additional time beyond that which is reasonable for carrying out enforcement and investigative actions. The development and distribution of critical messages and broadcasts regarding the child victims in these cases should not be delayed due to the process of requesting the activation of an AMBER Alert.

Law enforcement agencies must understand how AMBER Alert core activation and notification elements impact their operations

when these incidents occur. Agency staff who coordinate training should work proactively with their state and/or regional AMBER Alert Coordinators to ensure that personnel have the training and operational tools they need to support a functional, working knowledge of how the AMBER Alert process works in their area.

Understanding how AMBER Alerts are requested, what information is needed to support the request, how activation is made, what information will be broadcast and included in other messaging, and how to update the AMBER Alert Coordinator and the media with new developments in the case – all of these components will make law enforcement personnel stronger and more confident contributors to their jurisdictions' AMBER Alert programs. Together, the work of law enforcement and the AMBER Alert program create the best possible chance to rescue endangered missing and abducted children and bring them home safely.

Threat Assessment Matrix .pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

[Madison County Sheriff's Office]

Threat Assessment Matrix

The Threat Assessment Matrix is designed to assist law enforcement personnel to identify and consider the totality of the known facts and circumstances to accurately assess the degree of threat potentially faced by law enforcement officers in situations where consultation with and/or use of a specially trained Crisis Response Team (CRT) may be warranted to safely conduct sensitive law enforcement operations. To complete: place an "X" in each applicable block. Next, place the numerical point value for each checked box in the "SCORE" column. Add the points in the Score column for a Total Score. Compare the total score to the score value below to determine necessary actions. For Search and Arrest Warrants, skip Section V – Calls for Service/Patrol Operations. For Calls for Service, skip Sections I and II.

FACT	X	POINTS	SCORE
I. Search Warrant			
Search Warrant is for evidence of property crimes only	☐	0	
Search Warrant is for evidence of narcotics violations (possession or distribution)	☐	2	
Search Warrant is for evidence of violent crime(s)	☐	3	
Search Warrant is for explosives, weapons or other dangerous devices	☐	10	
Search Warrant is "Knock and Announce"	☐	1	
II. Arrest Warrant			
Arrest Warrant is for property crimes only	☐	0	
Arrest Warrant is for narcotics violations (possession, distribution, or manufacture)	☐	5	
Arrest warrant is for weapons violations	☐	5	
Arrest warrant is for crimes of violence (misdemeanor)	☐	6	
Arrest Warrant is for crimes of violence (Felony)	☐	8	
III. Target Location			
Execution of warrant requires no forcible entry (or unknown)	☐	1	
Execution of warrant requires use of breaching tools (deadbolt locks)	☐	4	
Execution of warrant requires specialized breaching tools (fortifications)	☐	10	
Target location has dog(s) for protection	☐	5	
Target location has exterior video surveillance	☐	4	
Target location is not amenable to concealed approach	☐	3	
Target location is a multi-story building	☐	2	
IV. Known Subject of Warrant or Associated With Target Location			
Subject has history of property crimes only	☐	1	
Subject has history of narcotics use or possession only	☐	3	
Subject has history of narcotics sales, manufacture or distribution	☐	5	
Subject has history of violent crimes against persons or is a third-strike candidate	☐	8	
FACT	**X**	**POINTS**	**SCORE**
Subject has history of assaultive behavior against police	☐	10	

Subject has made threats of violence	☐	4	
Subject has a known mental health condition	☐	4	
Subject has used firearms during the commission of crime(s)	☐	10	
Subject is currently on probation or parole	☐	3	
Subject is associated with violent criminal organization (militia, gang, terrorist, extremist, etc.)	☐	8	
Subject is known to possess firearms	☐	5	
Subject is known to possess automatic firearms	☐	8	
V. Calls for Service/Patrol Operations			
Subject has committed or is suspected of a misdemeanor crime against property	☐	0	
Subject has committed or is suspected of a felony crime against property	☐	7	
Subject has committed or is suspected of a misdemeanor crime against person(s)	☐	3	
Subject has committed/is suspected of a felony crime against person(s)	☐	6	
Subject is barricaded and suicidal	☐	10	
VI. Mandatory Crisis Response Unit Consult			
Target location contains suspected explosives, weapons, or other dangerous devices	☐		
Search or Arrest warrant for Suspect of a homicide	☐		
VII. Mandatory Virginia State Police Tactical Team			
Target location is heavily fortified and/or booby trapped	☐		
Target location has armed countersurveillance personnel on site	☐		
Barricaded Subject in Possession of Firearm	☐		
Search Warrant is for suspected clandestine drug lab/production facility	☐		
		TOTAL SCORE	

KEY:

1-12 points: **Handle with investigative/patrol personnel.**
12-25 points: **Handle with Crisis Response Unit.**
25+ points: **Use of State Police Tactical Team.**

Case Number

Case Officer: _____ **Supervisor:** _____ **Date:** _____

CRU Commanding Officer: _____ **Consult** ☐ **Approved** ☐ **Declined** ☐ **Date:** _____

Comments: _____

_____

_____

_____

_____

_____

VA Madison County Child Abuse Multi-Disciplinary Team (MDT Agreement July 1 2020.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

MADISON COUNTY CHILD ABUSE MULTI-DISCIPLINARY TEAM (MDT)

MEMORANDUM OF AGREEMENT

July 1, 2020

I. Purpose

The goal of the Madison County Multi-Disciplinary Team ("MDT") is to enhance the community's response to incidents of child abuse and neglect and/or child-involved sexual abuse through collaboration between agencies. This Memorandum of Agreement outlines the investigation protocol for child abuse cases and the MDT case review process.

In accordance to §§ 15.2-1627.5, 63.2-1503(K), and 63.2-1507 of the Code of Virginia, the undersigned agencies agree to collaborate through a MDT by conducting regular case reviews of new and ongoing reports of felony sex offenses in Madison County involving a child, as well as other reports of child abuse and neglect as appropriate.

II. Membership and Meeting Attendees

Membership in the MDT will be comprised of:

1. Commonwealth's Attorney's Office for County of Madison
2. Madison County Sheriff's Office ("Sheriff's Office")
3. Madison County Victim/Witness Program
4. Madison County Department of Social Services
5. Foothills Child Advocacy Center

In addition to the member agencies and organizations, there are other community stakeholders whose presence at the MDT meetings would further the goals of creating a comprehensive community response and greater collaboration between agencies. Such agencies and organizations are encouraged to attend the MDT meetings and shall abide by the confidentiality required in this Agreement and other applicable laws and regulations. Examples of such community stakeholders who are not members of the MDT but whose participation is valuable to the MDT's goals include Madison County Public Schools ("MCPS"), Juvenile Court Services Unit ("CSU"), Services to Abused Families ("SAFE"), the Rappahannock Rapidan Community Services Board ("RRCSB"), and the University of Virginia Medical Center Forensic Team.

III. Confidentiality

The MDT meetings shall take place under strict confidentiality. Members acknowledge their responsibility under state law to maintain strict confidence with case information shared during meetings. Confidentiality forms shall be signed by MDT members prior to each MDT meeting and such confidential information discussed shall not be shared outside of the meeting other than with the Primary Investigative Team and/or parties deemed by the Primary Investigative Team for purposes of a petition action, criminal prosecution, or other intervention deemed appropriate by the Primary Investigative Team.

"*Primary Investigative Team*" shall mean the MDT members working on a specific case, typically comprised of a law enforcement investigator, a Child Protective Services ("CPS") investigator, prosecutor, and a victim/witness support professional.

IV. Meetings

As a matter of course, Madison County MDT meetings will take place at the Office of the Commonwealth's Attorney, 15 Court Square, Madison, Virginia 22727 at 9:00 a.m. on the last Friday of each month. Adjustments in scheduling may be made to accommodate holiday schedules or other conflicts. Each meeting shall be coordinated by the Commonwealth's Attorney or her designee. The agenda for each meeting will generally include:

1. Signing of Confidentiality Agreement
2. Review of Existing Cases
3. Review of New Cases
4. General Discussion of Response Policies and Protocols

The MDT coordinator will prepare and transmit via confidential means such as email a list of existing cases expected to be presented at the upcoming MDT meeting. MDT members with new cases shall provide in advance to the coordinator a list of new matters to be discussed at the next available meeting. The lead investigator with law enforcement or CPS, in each case shall give an oral presentation on the facts of each case, evidence that has been developed, child protection issues, and a suggested response.

Individual cases will be reviewed by the MDT at every meeting until the pending investigation is completed by a final finding by CPS, prosecution is completed, or the charge is determined to be unfounded.

V. Investigation Protocol

Each agency will work within its existing policies and procedures in the investigation of child abuse cases. Nothing in this investigation protocol supersedes any statutes, rules, and regulations governing each agency.

A. Initiation and Notification

1. Where initial complaint is to CPS

Pursuant to Code of Virginia § 63.2-1503(D), CPS shall upon receipt of a complaint, report it immediately (but in no case more than two hours of receipt) to the Commonwealth's Attorney and the Sheriff's Office and make available their records when abuse or neglect is suspected in any case involving:

a) Death of a child;
b) Injury or threatened injury to the child in which a felony or Class 1 misdemeanor is also suspected;
c) Any sexual abuse, suspected sexual abuse or other sexual offense involving a child, including but not limited to the use or display of the child in sexually explicit visual material, as defined in § 18.2-374.1;
d) Any abduction of a child;
e) Any felony or Class 1 misdemeanor drug offense involving a child; or
f) Contributing to the delinquency of a minor in violation of § 18.2-371.

Where feasible, such notification shall be transmitted via email simultaneously to the following persons: the Commonwealth's Attorney and her deputy; the Lieutenant of the Criminal Investigations Division with the Sheriff's Office; the CPS supervisor, CPS investigators, and any designated intake personnel at DSS; and any other persons/agency representative that is anticipated will become part of the Primary Investigative Team.

After the complaint referral from CPS is screened by the Sheriff's Office for validity, the Sheriff's Office shall assign a lead investigator to the matter. The lead investigator shall coordinate with the assigned CPS worker to develop a preliminary plan for the investigation, including the scheduling of medical examinations and forensic interviews, as appropriate. The Sheriff's Office shall keep the Commonwealth's Attorney apprised of case developments.

2. Where initial complaint is to the Sheriff's Office

When the initial report of child abuse or neglect is received by the Sheriff's Office, the responding officer to the initial call will gather preliminary information regarding the complaint and validate whether the situation necessitates the notification and involvement of CPS. Pursuant to Code of Virginia § 63.2-1509(A)(8), when a law enforcement officer has reason to suspect that a child is an abused or neglected child, the officer shall report the matter immediately to CPS. Such notification should include the names and date(s) of birth of children, and contact information for parent(s) or guardian(s) of the children. Also pursuant to Code of Virginia § 63.2-1509(A), the Sheriff's Office shall disclose all information that is the basis of the suspicion of abuse or neglect of the child, and upon request by CPS, shall make available to CPS any information, records, or reports that document the basis for the report. Any criminal investigative reports received by CPS from law-enforcement agencies shall not be further disseminated by the investigating agency nor shall they be subject to public disclosure.

If the responding officer or other law enforcement validates the initial complaint, the Sheriff's Office shall assign a lead investigator to the matter and notify the Commonwealth's Attorney that an investigation is commencing. The lead investigator shall coordinate with the assigned CPS worker to develop a preliminary plan for the investigation, including the scheduling of medical examinations and forensic interviews, as appropriate. The Sheriff's Office shall keep the Commonwealth's Attorney apprised of case developments.

B. Interviews

1. Order of Interviews

The Primary Investigative Team will decide on a case-by-case basis the order in which it will interview the relevant parties to an investigation. Forensic interview protocol recommends interviewing the relevant parties in the following order:

a) Source of report (particularly where source is non-offending caretaker).
b) Child victim(s)
c) Siblings or other child witnesses

d) Non-offending caretaker
e) Other witnesses/collateral witnesses
f) Alleged perpetrator

2. Forensic Interview

A forensic interview will be conducted for all alleged child victims of sexual abuse, severe physical abuse and child witnesses to violent crime. Forensic interviews shall be conducted primarily at the Madison County Forensic Interview Room located in the Commonwealth's Attorney's Office by a trained forensic interviewer, where practicable for the victim and the primary investigation team. Forensic interviews at the Madison County Forensic Interview Room shall be performed in accordance with the CAC's National Children's Alliance accreditation standards.

3. Forensic Medical Examinations

Forensic medical examinations shall as a matter of course be made available to child victims of physical abuse. Emergent medical examinations shall be as soon as practicable made available to child victims where there is a concern for acute physical trauma. In order to reduce anxiety for the child and family, information about what will happen during the medical exam should be provided to the non-offending caregiver when a medical appointment is scheduled. Properly trained medical professionals will perform evaluations of possible child abuse in a safe, neutral, and child-friendly environment. Children in MDT cases will have access to appropriate medical evaluation and treatment regardless of their ability to pay for services.

If an allegation indicates that sexual abuse occurred within the past 120 hours (five days), an examination should be immediately made available to the child. If the abuse is not acute (more than 120 hours) the child should be referred as soon as possible to a suitable facility with staff trained in specialized evaluations for abuse. Obtaining a medical history from the child may include non-leading questions regarding abuse, but should not duplicate the full investigative interview conducted with the child.

4. Audio/Videotaping of Interviews

When possible, all interviews of child victims, suspected abusers, and other relevant witnesses to the abuse or neglect shall be recorded by video and/or audio. If any party refuses to be interviewed on tape or video, or is not in the best interest of a child victim, the Primary Investigative Team shall nevertheless conduct the interview in the absence of a recording device.

5. Alleged Abuser Interview

Generally, law enforcement investigators shall be considered the lead interviewer in the interviewing of a suspect. When possible, CPS and other interested parties should observe the interview of the alleged suspect and be allowed to have specific questions asked of the suspect. Flexibility of the roles of law enforcement and DSS/CPS is permitted in situations where it would strengthen the investigation.

6. CPS or Sheriff's Office Determinations

At any point in the investigatory process where appropriate, the lead investigator from the Sheriff's Office may determine that the matter being investigated is not criminal in nature and decide that the Sheriff's Office need not participate in any further joint investigation.

Where appropriate, the lead investigator from CPS may determine that the alleged abuse does not rise to the level of any violation of DSS regulations and guidelines and may finalize their investigation under their agency's guidelines and decide that CPS need not participate in any further joint investigation.

C. Case Decision-Making

When all available information is gathered, the Primary Investigative Team will determine if there is evidence to substantiate that the child has been abused, who the abuser is, and if there is substantial evidence to make a CPS finding and/or pursue criminal charges.

The substantiation process pulls all of the evidence together, including that which supports and refutes the allegation. The decision should be based on the following classes of evidence:

a) The child's statement;
b) Statements of other witnesses, including other children, non-offending caretakers, and other professionals;
c) Medical findings;
d) Physical and corroborating evidence;
e) Behavioral indicators;
f) Any relevant psychological information involving the child, family, or alleged perpetrator; and
g) The statement of the alleged perpetrator.

1. CPS Intervention

CPS may make a finding of child abuse based on the legal standard of preponderance of the evidence. It is the responsibility of the CPS investigator to determine the immediate safety needs of the child and to plan with caretakers to ensure the continuing safety of the child. The written safety plan outlines what the caretaker needs to do to keep the child safe and is signed by the CPS Investigator and one or both caretakers. The CPS investigator may also petition the Juvenile and Domestic Relations court for a protective order if high risk to the child exists (for example, asking the court to order no contact with the abuser).

If there is evidence that establishes an immediate threat to the life or health of the child, which cannot be resolved through safety planning, the CPS investigator may petition the court for the emergency removal of the child from the home, or under imminent risk of harm assume emergency custody prior to court intervention. When CPS petitions for a

protective order or a removal order, a preponderance of the evidence must be presented so that the court makes a finding of abuse or neglect.

The CPS investigator may refer the family to receive ongoing child protective services so that a social worker is assigned to help the family coordinate services that increase the protective factors to the child.

2. Criminal Charges

After considering the totality of the evidence during the decision-making stage, the Sheriff's Office and Commonwealth's Attorney will determine if sufficient evidence exists to press criminal charges, and the legal process to initiate the charges (e.g. via warrant of arrest or direct indictment). The legal standard of probable cause is needed to file criminal charges. The evidentiary standard of beyond a reasonable doubt is required to successfully prosecute a criminal case.

In every feasible instance, the Sheriff's Office shall consult with the Commonwealth's Attorney regarding charges pertaining to child abuse prior to the obtaining of arrest warrants. If it is the determination of the Sheriff's Office that an arrest should be made immediately due to safety or other concerns, the Sheriff's Office shall effectuate the arrest and notify the Commonwealth's Attorney forthwith regarding the charges.

After charges are initiated, the Sheriff's Office and CPS will provide timely updates and additional information regarding the case to the assigned prosecutor as they become available. The Commonwealth's Attorney's office, Sheriff's Office, and CPS will also coordinate the referral of cases to the Victim/Witness Coordinator.

3. Victim/Witness Support

The Victim/Witness coordinator shall assist in offering services to victims and their families through the investigation and any subsequent relevant legal process, to include providing:

a) Information regarding the custody status of the accused;
b) Information about the court process and the steps a case will take as it progresses through the criminal justice process;
c) An explanation of the Virginia Victim's Rights Act;
d) Notification of court dates;
e) Assistance with restitution including assistance with filing claims with the Criminal Injuries Compensation Fund;
f) Referrals for counseling and other community resources as appropriate;
g) Support surrounding and, where appropriate, accompaniment to forensic interviews, forensic medical exams, court hearings and meetings with the Commonwealth's Attorney;
h) Assistance with the preparation with Victim Impact Statements for court presentation; and
i) Tours of the courtroom prior to court appearances.

D. Conclusion of Cases

Following the conclusion of a DSS investigation or criminal prosecution, the Primary Investigative Team on the case should report the final result of the case to the full MDT. Regular MDT meetings should be a forum for discussion of lessons learned from concluded cases such that improvements can be made to future investigations.

(Endorsements on following page)

ENDORSEMENTS

The following parties agree to adhere to the terms of this Agreement:

Commonwealth's Attorney's Office for County of Madison

By: _____ 6/23/20

Title: Commonwealth's Attorney Date

Madison County Sheriff's Office

By: E J Weaver 6/24/2020

Title: SHERIFF, MADISON CO. Date

Madison County Victim/Witness Program

By: _____ 6/23/2020

Title: Director Madison Victim/Witness Date

Madison County Department of Social Services

By: Valerie Ward 6/26/2020

Title: Director, Madison DSS Date

Foothills Child Advocacy Center

By: Cynthia F. Hurst 6/3/20

Title: Executive Director Date

316 HIPAA Compliant Medical Records Release Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

HIPAA COMPLIANT AUTHORIZATION FOR THE RELEASE OF PATIENT INFORMATION PURSUANT TO 45 CFR 164.508

TO: _____
Name of Healthcare Provider/Physician/Facility/Medicare Contractor

_____
Street Address

_____
City, State and Zip Code

RE: Patient Name: _____

Date of Birth: _____ Social Security Number: _____

I authorize and request the disclosure of all protected information for the purpose of review and evaluation in connection with a legal claim. I expressly request that the designated record custodian of all covered entities under HIPAA identified above disclose full and complete protected medical information including the following:

☐ All medical records, meaning every page in my record, including but not limited to: office notes, face sheets, history and physical, consultation notes, inpatient, outpatient and emergency room treatment, all clinical charts, r ports, order sheets, progress notes, nurse's notes, social worker records, clinic records, treatment plans, admission records, discharge summaries, requests for and reports of consultations, documents, correspondence, test results, statements, questionnaires/histories, correspondence, photographs, videotapes, telephone messages, and records received by other medical providers.

☐ All physical, occupational and rehab requests, consultations and progress notes.

☐ All disability, Medicaid or Medicare records including claim forms and record of denial of benefits.

☐ All employment, personnel or wage records.

☐ All autopsy, laboratory, histology, cytology, pathology, immunohistochemistry records and specimens; radiology records and films including CT scan, MRI, MRA, EMG, bone scan, myleogram; nerve conduction study, echocardiogram and cardiac catheterization results, videos/CDs/films/reels and reports.

☐ All pharmacy/prescription records including NDC numbers and drug information handouts/monographs.

☐ All billing records including all statements, insurance claim forms, itemized bills, and records of billing to third party payers and payment or denial of benefits for the period _____ to _____.

I understand the information to be released or disclosed may include information relating to sexually transmitted diseases, acquired immunodeficiency syndrome (AIDS), or human

immunodeficiency virus (HIV), and alcohol and drug abuse. I authorize the release or disclosure of this type of information.

This protected health information is disclosed for the following purposes: _____

_____

This authorization is given in compliance with the federal consent requirements for release of alcohol or substance abuse records of 42 CFR 2.31, the restrictions of which have been specifically considered and expressly waived.

You are authorized to release the above records to the following representatives of defendants in the above-entitled matter who have agreed to pay reasonable charges made by you to supply copies of such records:

_____

Name of Representative

_____

Representative Capacity (e.g. attorney, records requestor, agent, etc.)

_____

Street Address

_____

City, State and Zip Code

I understand the following: See CFR §164.508(c)(2)(i-iii)

a. I have a right to revoke this authorization in writing at any time, except to the extent information has been released in reliance upon this authorization.
b. The information released in response to this authorization may be re-disclosed to other parties.
c. My treatment or payment for my treatment cannot be conditioned on the signing of this authorization.

Any facsimile, copy or photocopy of the authorization shall authorize you to release the records requested herein. This authorization shall be in force and effect until two years from date of execution at which time this authorization expires.

_____ _____

Signature of Patient or Legally Authorized Representative Date
(See 45CFR § 164.508(c)(1)(vi))

_____

Name and Relationship of Legally Authorized Representative to Patient
(See 45CFR §164.508(c)(1)(iv))

_____ _____

Witness Signature Date

316 Missing Child School Notification Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

MADISON COUNTY SHERIFF'S OFFICE
EMERGENCY SCHOOL NOTIFICATION
MISSING OR ABDUCTED CHILD ALERT

Date of notification: _____ **Case No.** _____

Notice to the school administration of (School Name) _____

Name of missing / abducted child:_____

Sex _____ Race _____ Date of Birth_____

If this student is located, or if anyone calls asking for information, or requests the transfer of school records, immediate law enforcement notification is required.

Do not release any information or records until told to do so by law enforcement. Do not tell the requesting party of this notification, law enforcement will instruct you what to do. Immediately contact:

Investigating Officer: _____ **Badge/ID No.**_____

Telephone: _____

- In you are unable to make personal contact with the investigating officer in this matter, immediately contact the on-duty supervisor and reference this notification sheet. The phone numbers are:

  Investigations Lieutenant_____

  Patrol Lieutenant _____

- If the child is found during off-hours, or no one answers the phone number listed above, call 911 and provide the information above.

Photograph

If available, a recent photograph of the missing child is attached to this notification. School authorities may have a more recent photograph. If so, please notify the investigating officer.

☐ Photograph not provided by reporting party.

See back page for additional information / instructions

All law enforcement agencies are required to notify the missing child's school of attendance, in writing, within the (10) days of the date upon which the child is reported missing or abducted. The school should place this notification letter in the front of the student's school / attendance record.

This notification form has two purposes:

(1) In many cases, young children in elementary school fall victim to parental abduction, or other related serious victimization / kidnapping. When this occurs, many times the abductor will have to request the previous school records in order to enroll the child into a new school.

(2) Sometimes, in cases where a child has run away, he/she may return to school without notifying the parents.

By having this form in the front of the child school / attendance record, the school can be made aware of the situation and cause law enforcement authorities to be notified immediately, potentially aiding in the recovery of the child.

Upon the initial enrollment of a pupil in a public or private elementary school; or whenever an elementary school pupil (a) transfers from one school district to another, (b) transfers to an elementary school within the same district, (c) transfers from one private elementary school to another, (d) transfers from a private elementary school to a public elementary school, or (e) transfers from a public elementary school to a private elementary school, the principal of the school that the child enters or to which he or she transfers is urged to check to see if the child may resemble a child listed as missing by the National Center for Missing & Exploited Children© (NCMEC) online at https://www.missingkids.org/gethelpnow/search. A U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention partner, the National Center for Missing & Exploited Children© (NCMEC) serves as an information clearinghouse and national resource center on issues related to victims, missing and exploited children and operates a national, toll-free 24-hour hotline at 800-THE-LOST© or 1-(800)-843-5678.

If a school receives a record inquiry or request from any person or entity for a missing child about whom the school has been notified, the school should immediately notify the law enforcement authorities who informed the school of the missing child's status.

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN®
www.missingkids.org

316 Investigative checklist for Missing Children.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN®

INVESTIGATIVE CHECKLIST FOR FIRST RESPONDERS

This checklist is meant to provide a framework of recommended actions, considerations, and activities to perform competent, productive, and thorough missing/abducted children investigations with the goal of better assisting families, victims, and the community.

FIRST RESPONDER

- ☐ Activate body camera or vehicle mounted camera, if circumstances and policy allow.
- ☐ Interview parent(s)/guardian(s)/person who made the initial report.
- ☐ Confirm the child is in fact missing.
- ☐ Identify the circumstances of the missing episode.
- ☐ Determine when, where, and by whom the missing child was last seen.
- ☐ Interview the individuals who last had contact with the child.
- ☐ Identify the child's zone of safety for his or her age and developmental stage. Determine if the case involves a child with special needs. If so, *see Investigative Checklist for Law Enforcement When Responding to Missing Children With Special Needs.*
- ☐ Make an **initial assessment**, based on the available information, of the type of incident whether nonfamily abduction; family abduction; runaway; or lost, injured, otherwise missing, or a child with special needs.
- ☐ Children on the autism spectrum are at high risk. Immediately call for additional responders, search nearby bodies of water, and notify a supervisor.
- ☐ Obtain a **detailed** description of the missing child, abductor, and any vehicles used.
- ☐ Secure recent photos/videos of the missing child/abductor.
- ☐ Evaluate whether the circumstances meet **AMBER Alert criteria** and/or other immediate community notification protocol if not already activated. Discuss plan activation with supervisor.
- ☐ Advise the left-behind parent, in suspected family abduction, to call NCMEC and if any chance the child may be taken outside the United States, the parent should also contact the U.S. Department of State's Office of Children's Issues to report a potential kidnapping. Do not presume the child is safe.
- ☐ Determine the need for external, rapid deployment support, such as:
  - ○ FBI's Child Abduction Rapid Deployment (CARD) team
  - ○ Local or regional Child Abduction Response Teams (CARTs)
  - ○ NCMEC's Team Adam
- ☐ Relay detailed descriptive information to communications unit for broadcast updates.
- ☐ Determine need for additional personnel including investigative and supervisory staff.
- ☐ Brief and update all additional responding personnel.
- ☐ Obtain and note consent to search home or building where incident took place **even if the premises have been previously searched by family members or others**.
- ☐ Conduct an immediate, thorough search of the missing child's home **even if the child was reported missing from a different location**.
- ☐ Inquire if the child has access to the internet and evaluate its potential role. Do not overlook activity on social media accounts or other online apps and platforms.

Copyright © 2004-2020 National Center for Missing & Exploited Children. All rights reserved.

- [ ] Identify and separately interview everyone at the scene. Make sure their interview and identifying information is properly recorded. To aid in this process, if possible, take pictures or record video images of everyone present. Vehicle mounted or body cameras may be helpful with this task.
  - ◯ Note name, address, home/business phone numbers of each person.
  - ◯ Determine each person's relationship to the missing child.
  - ◯ Note information each person may have about the circumstances surrounding the missing episode.
  - ◯ Determine when/where each person last saw the child.
  - ◯ Ask each one, "What do you think happened to the child?"
  - ◯ Obtain names/addresses/phone numbers of the child's friends/associates and other relatives and friends of the family.
  - ◯ Determine if any suspicious activity or people were seen in the area.
  - ◯ Determine if any people were seen who seemed unusual, strange, or out-of-place.
  - ◯ Continue to keep communications unit apprised of all appropriate developing information for broadcast updates.
- [ ] Seal/protect scene and area of the child's home, including the child's personal articles such as hairbrush, diary, photos, and items with the child's fingerprints/footprints/teeth impressions. Determine if any of the child's personal items are missing. If possible, photograph/take videos of these areas.
- [ ] Evaluate the contents and appearance of the child's room/residence.
- [ ] Ascertain if the child has a cellphone or other electronic communication device and obtain the most recent records of their use.
- [ ] Extend search to surrounding areas and vehicles, including those abandoned, and other places of concealment such as abandoned appliances, pools, wells, sheds, or other areas considered to be "attractive nuisances."
- [ ] Treat areas of interest as potential crime scenes including all areas where the child may have been or was going to be located.
- [ ] Determine if surveillance or security cameras in the vicinity may have captured relevant information.
- [ ] Review sex offender registries to determine if registered individuals live/work in the area or might otherwise be associated with the case. Call NCMEC at 1-800-THE-LOST® (1-800-843-5678) to request assistance with this step.
- [ ] Interview other family members, friends/associates of the child, and friends of the family to determine:
  - ◯ when each last saw the child.
  - ◯ what they think happened to the child.
  - ◯ if the child had complained about being approached by anyone.
  - ◯ child's social networking accounts and usernames.
  - ◯ if the child utilizes chat apps on their cellphone.
  - ◯ if the child has mentioned meeting anyone online.
- [ ] Ensure information regarding the missing child is entered into the National Crime Information Center's (NCIC) Missing Person File **no more than two hours after receipt of the report** and any information about a suspected abductor is entered into the NCIC Wanted Person File. Ensure the entry includes a Child Abduction (CA) flag if appropriate.
- [ ] Prepare missing child poster/flier with the child/abductor's photo and descriptive information. Distribute in appropriate geographic regions. Call NCMEC at 1-800-THE-LOST® (1-800-843-5678) for assistance with this step.
- [ ] Prepare reports/make all required notifications.

Copyright © 2004-2020 National Center for Missing & Exploited Children. All rights reserved.

SUPERVISORY OFFICER

- [ ] Obtain briefing and written reports from the first responding officer and other personnel at the scene. Call and report the case to the National Center for Missing & Exploited Children (NCMEC).
- [ ] Decide if circumstances meet the protocol in place for activation of an **AMBER Alert** and/or other immediate community notification systems, if not already activated.
- [ ] Determine if additional personnel are needed to assist in the investigation.
- [ ] Establish a command post away from the child's residence.
- [ ] Review responding officer recommendations for additional resources. Consider further support from:
  - ◯ State/Territorial Police
  - ◯ Missing Child Clearinghouse
  - ◯ Federal Bureau of Investigation (FBI)
  - ◯ Specialized Units
  - ◯ Victim-Witness Services
  - ◯ United States Marshals Service (USMS)
- [ ] Confirm all the required resources, equipment, and assistance necessary to conduct an efficient investigation have been requested and expedite their availability.
- [ ] Ensure coordination/cooperation among all law enforcement personnel involved in the investigation and search effort.
- [ ] Verify all required notifications are made.
- [ ] Ensure all agency policies and procedures are in compliance.
- [ ] Be available to make any decisions or determinations as they develop.
- [ ] Use media including print, radio, television, and the internet/social media to assist in the search throughout the duration of the case.
- [ ] Collaborate with your agency's communications team (PIO/PAO) to disseminate information appropriately to the public. Designate a representative to coordinate public communications if your agency does not have one.

Copyright © 2004-2020 National Center for Missing & Exploited Children. All rights reserved.

INVESTIGATIVE OFFICER

- ☐ Obtain briefing from the first responding officer and other on-scene personnel.
- ☐ Verify the accuracy of all descriptive information and other details developed during the preliminary investigation.
- ☐ Initiate a neighborhood canvass using a standardized questionnaire.
- ☐ Obtain a brief, recent history of family dynamics.
- ☐ Determine if social services or child protective services have been or are currently involved with the family.
- ☐ Correct and investigate the reasons for conflicting information offered by witnesses and other individuals.
- ☐ Provide relevant items and materials secured from the scene(s) to specialized units and external support agencies as need to aid in searches.
- ☐ Review and evaluate all available information and evidence collected.
- ☐ Secure the child's latest medical and dental records and items suitable for DNA collection.
- ☐ Contact landfill management and request they delay or at least segregate garbage and dumping containers from key investigative areas in cases where it is suspected there may be imminent danger to the missing child.
- ☐ Develop and execute an investigative plan.
- ☐ Conduct a criminal history background check on all principal suspects, witnesses, and participants in the investigation.
- ☐ Determine what additional resources and specialized services are required.
- ☐ Ensure details of the case have been reported to NCMEC. If the child is missing from placement, NCMEC is to be notified within 24 hours. The investigating agency, child welfare agency, and NCMEC are to maintain close liaison for the exchange of information and technical assistance.
- ☐ Prepare and update bulletins for local law enforcement agencies, missing child clearinghouse, FBI, and other appropriate agencies.
- ☐ Establish a phone hotline for receipt of tips and leads. Consider establishing an email address and other methods of electronically receiving leads as well.
- ☐ Establish a leads management system to prioritize leads and help ensure each one is reviewed and followed-up. Request support with this from NCMEC if needed.

This checklist is adapted from and to be used as a supplement to *Missing and Abducted Children: A Law-Enforcement Guide to Case Investigation and Program Management*. That guide contains additional recommended checklists and materials and may be downloaded free of charge at MissingKids.org/ourwork/publications. To request a free copy or assistance for specific cases, call **NCMEC at 1-800-THE-LOST® (1-800-843-5678)**. This project was supported by Grant No. 2019-MU-MU-K012 awarded by the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. This document is provided for informational purposes only in support of NCMEC's mission to serve as a resource center for law enforcement, families, and the public to help find missing children, reduce child sexual exploitation, and prevent child victimization and does not constitute legal advice or professional opinion about specific facts. Information provided in this document may not remain current or accurate, so recipients should use this document only as a starting point for their own independent research and analysis. If legal advice or other expert assistance is required, the services of a competent professional should be sought. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice. Copyright © 2004-2020 National Center for Missing & Exploited Children. All rights reserved. National Center for Missing & Exploited Children® and are registered trademarks of the National Center for Missing & Exploited Children. The AMBER Alert logo is a registered trademark of the U.S. Department of Justice. NCMEC Order #88.

Copyright © 2004-2020 National Center for Missing & Exploited Children. All rights reserved.

316 Missing Persons Investigation Checklist.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Missing Persons Checklist

If you think a person is missing, the following are actions that you can take.

- ☐ Immediately contact your local law enforcement agency to report the person missing. If the person went missing somewhere else, you may contact the law enforcement agency in that area. When you contact police, tell them that you need to file a missing persons' report.
- ☐ When you file a missing person's report the police will ask you a number of questions. It would be helpful if you had the following information. Do not worry; you need not delay contacting the police if you do not have all of the information below
  - a) Basic information about the Missing Person
    - ☐ Full name
    - ☐ Date of birth
    - ☐ Birthplace
    - ☐ Nicknames, if any
    - ☐ Current and previous addresses. Who else lived there?
    - ☐ Current and former employers.
  - b) Physical description of the Missing Person
    - ☐ Height
    - ☐ Weight
    - ☐ Age
    - ☐ Build
    - ☐ Hair Color/Length of Hair
    - ☐ Eye color?
    - ☐ Any Markings – such as tattoos, birthmarks, scars, etc.
    - ☐ Beard/Mustache/Sideburns
    - ☐ Find the most recent photo of the missing person
  - c) Habits and Personality of Missing Person
    - ☐ Does the person smoke? If yes, what brand of cigarettes? Does the person drink alcohol? If yes, what type?
    - ☐ Does the person use recreational drugs?
    - ☐ Does the person chew gum?
    - ☐ What type of recreation or activities does the person engage in including hobbies?
    - ☐ Are there novel habits that the person has? For instance, does the person have a place where they always go for coffee?
    - ☐ Does the person have particular banking habits?
    - ☐ What type of personality does the person have? Is the person outgoing or quiet? Is the person friendly or depressed?
    - ☐ What are the values and philosophy of the person?
    - ☐ Is the person religious?
    - ☐ Does the person have any emotional problems?
    - ☐ What level of education or training does the person have?
    - ☐ Does the person go to any particular areas, bars, taverns or places of interest?

d) Clothing that the Missing Person was wearing the last time seen
   - ☐ Style and color of shirt
   - ☐ Style and color of pants
   - ☐ Style and color of jacket or outerwear
   - ☐ If applicable, type of headwear
   - ☐ Type of glasses
   - ☐ Type of gloves
   - ☐ Type of footwear

e) Trip Plans of the Missing Person the day they went missing
   - ☐ What were the missing person's plans and/or activities on the day they went missing?
   - ☐ Where was he/she going?
   - ☐ Why was he/she going there?
   - ☐ Was the person traveling by car? If so, provide the make and model number, license plate number and registration.
   - ☐ Does the person have access to any other vehicles or mode of travel?

f) Information about the last time the Missing Person was seen
   - ☐ The time and location of where he/she was last seen
   - ☐ The name of the person who last saw the missing person
   - ☐ The name of the person who last talked at length with the missing person
   - ☐ The direction the missing person was traveling the last time seen.
   - ☐ The attitude of the missing person the last time seen
   - ☐ Was the missing person concerned about anything before he/she went missing?

g) Overall health and condition of the missing person
   - ☐ Physical condition
   - ☐ Any known medical problems.
   - ☐ Is the person suffering from Alzheimer's disease/dementia/memory loss? If so, are they registered on Safely Home? If they are registered on Safely Home, what is their registration number? Are they wearing a Safely Home identification bracelet or carrying an identification card?
   - ☐ Any handicaps or disabilities.
   - ☐ Any psychological problems
   - ☐ Any medications that the person is taking
   - ☐ Any addictions that the person has
   - ☐ Provide the name of the missing person's family physician and their health card number, if possible
   - ☐ Provide the name of the missing person's main dentist, if possible.

h) Potential People that the person would contact
   - ☐ List all of the people who the missing person may try to contact. Try to include addresses and telephone numbers.

☐ When the missing person's report has been filed, ask the police for the missing person's file number. As well, ask for contact information for the investigator in charge of the file.

- ☐ Secure the personal belongings and living space of the missing person until the police provide further direction. Below is a list of items of importance.
    - ☐ Items such as a hairbrush, a toothbrush, or undergarments. Investigators may need to undertake DNA analysis.
    - ☐ Any electronic equipment such as a cell phone or computer. What is the make of phone and the cell phone provider. As well, do you know if they were active on a chat line or other social on-line network such as MSN facebook?
    - ☐ Any personal documents such as banking statements and credit card statements as well as all bank card information.
    - ☐ Any written material such as a journal
- ☐ To make things more manageable, start a log or journal. Include all information about the missing person's case in the journal.
- ☐ The Police will likely request that there be one family contact with the police. This simplifies contact between the Police and the family. Police officers will only have to update one person about the investigation. In addition, they will know who to contact when information is needed from the family. Talk with your family and close friends about who will be the family contact. The members of your family may not want to take on this role. If so, you may decide that a close friend should be the contact person.
- ☐ If the missing person is a child, contact Child Find. They offer a 24 hour, 7 day per week toll free phone line to handle emergency situations. They can help with investigations and ground search assistance as well as making a poster.

<u>Actions your family can undertake</u>

- ☐ Conduct a telephone search. Phone friends and family that may have some idea of where the missing person is. Start with those closest to the missing person and write all of the information down in your journal.
- ☐ If you find out any additional information from telephone inquiries pass it on to police
- ☐ Put up flyers with a photograph of the missing person around your community. If the missing person is a child talk to Child Find Saskatchewan about the services they provide for distributing pictures and posters.
- ☐ Tell all necessary people about the disappearance of the missing person. This may include the missing person's employer, their bank, and their doctor. If the missing person is a child you will need to contact the school they are attending.
- ☐ If necessary, arrange for the payment of the missing person's mortgage, rent or bills. You may require legal advice on how to proceed.

<u>Actions to Undertake to Take Care of Yourself and your Family</u>

- ☐ Ask yourself if you need to take an extended leave from work. If you do, talk to your employer about what options might be available.
- ☐ If you feel you need an extension on bill payments then ask about what options are available

- ☐ Try to eat, sleep, and exercise on a regular basis. Although you may not feel that you have time it is important to take care of yourself
- ☐ Try not to blame yourself for the disappearance of your loved one. Treat yourself with as much kindness as you can in these difficult times.
- ☐ Try to realize your limits. Be easy on yourself if you are unable to provide what is needed in all situations. You may, for instance, be unable to provide emotional support to all of the members of your family. Don't feel guilty about seeking counseling services to help your family deal with the wide range of emotions that are being experienced.
- ☐ Don't feel guilty if you have to return to work. This does not mean that you have given up on the search for your loved one.

SP-183_Va_Missing_Children_Info_Clearinghouse_Report.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

SP-183 (Rev. 01-01-2006)

VIRGINIA MISSING CHILDREN INFORMATION CLEARINGHOUSE REPORT

INVESTIGATING OFFICER:

Date/Time Reported To Law Enforcement: _____

Date Entered VCIN/NCIC: _____

VIC No.: _____

PART 1

*Agency Submitting Report:

ORI No.:

*Last Name: | First Name: | Middle Name: | Suffix: | *Sex: | Race:

*Place of Birth: | *Date of Birth: * | Date of Emancipation if under 18 yoa**:

*Height: Ft. In. | *Weight Lbs. | *Eye Color: ☐ Black ☐ Blue ☐ Maroon ☐ Green ☐ Brown ☐ Gray ☐ Hazel ☐ Unknown ☐ Multicolor ☐ Pink | *Hair Color: ☐ Black ☐ Blond ☐ White ☐ Sandy ☐ Brown ☐ Gray ☐ Red ☐

Complexion: ☐ Fair/Light ☐ Albino ☐ Ruddy ☐ Lt. Brown ☐ Black ☐ Dark ☐ Sallow ☐ Med. Brown ☐ Medium ☐ Olive ☐ Yellow ☐ Dark Brown

Scars, Marks, Tattoos, Piercings and Other Characteristics:

Fingerprint Classification:

Social Security Number:

Operator's License Number: | O.L. State: | Date of Expiration: | DNA: ☐ Yes ☐ No Location of DNA:

*Date of Last Contact:

*Originating Agency Case Number:

*Fingerprints Available: ☐ Yes ☐ No
Location of the Fingerprints:

*Photo Available: ☐ Yes ☐ No
Photo Received: ☐ Yes ☐ No
Photo sent to the State Police: ☐ Yes ☐ No

*Dental Records: ☐ Yes ☐ No
Location of the Dental Records:

Blood Type:

Circumcision: ☐ C ☐ N ☐ U

Footprint Available: ☐ Yes ☐ No
Location of the Footprints:

Body X-Rays Available: ☐ Full ☐ Partial ☐ No
Location of the X-Rays:

*Medication Required: ☐ Yes ☐ No
Medication Type:

*Name of School Last Attended:

*Code Number of School Last Attended:
Code No.:

County/City Code of Birth:
(Mandatory if POB is VA)

Mother's Maiden Name (if POB is VA):
Last: First : Middle:

*Telephone # of investigating agency (accessible 24 hours) :
Area Code ( ) -

*Authority for Release: ☐ Yes ☐ No
(Part IV)

Last Seen in Company of: NAME(S): | Sex: | Race:

(1)

(2)

*Name of Child's Parents or Legal Guardian: Name:
Address/City/State/Zip: Phone:

MISCELLANEOUS DATA: (Information which may assist in identification: child's nickname, associates, direction of travel, hairstyle, clothing, etc.)

VEHICLE INFORMATION:

License Plate Number: | State: | Year of Exp. : | Lic. Type: | VIN:

Vehicle Year: | Make: | Model: | Style: | Color:

Corrective Vision Prescription:

Jewelry Type and Description:

*** MANDATORY DATA ELEMENTS**

****Date of Emancipation is individual's eighteenth birth date. NOT NEEDED FOR CHILD 18 OR OLDER**

CHECK APPLICABLE CONDITION:

1. ☐ DISABILITY:

   Child missing is under proven physical/mental disability thereby subjecting herself/himself or others to personal or immediate danger.

2. ☐ ENDANGERED:

   Child missing under circumstances indicating his/her physical safety is in danger.

3. ☐ INVOLUNTARY:

   Child missing under circumstances indicating the disappearance was not voluntary.

4. ☐ JUVENILE:

   Child under 18 years of age who is missing and does not meet entry criteria set forth in #1, 2, or 3. This category should not include children under the age of 12

5. ☐ MISSING CHILD:

   Child between the age of 18 and less than 21 years of age who is missing and does not meet the criteria set forth in #1, #2, or #3, Child entered as Missing Person Other (Message Key EMO)

PART III

I certify the person described in Part I is missing and that the information I have furnished is true and correct to the best of my knowledge and belief.

Signature	Date	Relationship

PART IV

I authorize any law-enforcement official to use photographs and/or any other identifying information I have provided in any manner they deem necessary in attempting to locate the person I am reporting missing.

I represent that I am the natural parent and/or legal guardian of the person named in this report, and have the legal right to sign this authorization and consent.

Signature	Date	Relationship

Virginia Missing Children Information Clearinghouse
Virginia State Police
Criminal Justice Information Services Division
P. O. Box 27472
Richmond, Virginia 23261-7472

Distribution:

	Mailed Original	Mailed "Located" copy
Virginia Missing Children Clearinghouse	Date _____	Date _____
Local School Division Superintendent – 1	Date _____	Date _____
Registrar of Vital Records – 1	Date _____	Date _____
P. O. Box 1000		
Richmond, Virginia 23208-1000	By _____	By _____

Cleared VCIN/NCIC Date _____

PLEASE ATTACH A CURRENT PHOTOGRAPH OF THE MISSING CHILD TO THIS FORM

SP-067_Va_Missing_Adult_Info_Clearinghouse_Report.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

SP-67 (Rev. 1-1-2006)

VIRGINIA MISSING PERSON INFORMATION CLEARINGHOUSE REPORT

INVESTIGATING OFFICER

DATE REPORTED: _____
DATE ENTERED VCIN/NCIC: _____
VIC NO: _____

PART 1

*Agency Submitting Report: | *ORI No:

*Last Name | *First Name | Middle Name | Suffix | *Sex | *Race

Place of Birth: | *Date of Birth:

*Height: Ft. In. | *Weight: Lbs. | *Eye Color ☐ Black ☐ Blue ☐ Maroon ☐ Green ☐ Brown ☐ Gray ☐ Hazel ☐ Unknown ☐ Multicolor ☐ Pink | *Hair Color ☐ Black ☐ Blond ☐ White ☐ Sandy ☐ Brown ☐ Gray ☐ Red ☐ _____

Complexion ☐ Fair/Light ☐ Albino ☐ Ruddy ☐ Lt. Brown ☐ Black ☐ Dark ☐ Sallow ☐ Med. Brown ☐ Medium ☐ Olive ☐ Yellow ☐ Dark Brown

Scars, Marks, Tattoos and Other Characteristics

Fingerprint Classification: | Social Security Number:

Operator's License Number | O.L. State | Date of Expiration | DNA ☐ Yes ☐ No Location of DNA:

*Date of Last Contact | *Originating Agency Case Number

Fingerprints Available ☐ Yes ☐ No Location of the Fingerprints: | Photo Available ☐ Yes ☐ No Photo Received ☐ Yes ☐ No Photo sent to the State Police ☐ Yes ☐ No | Dental Records ☐ Yes ☐ No Location of the Dental Records:

Blood Type | Body X-Rays Available ☐ Full ☐ Partial ☐ No | Location of the X-Rays:

Medication Required ☐ Yes ☐ No | Medication Type | Medical Condition ☐ Yes ☐ No If Yes, what type:

Last Name | First Name | Middle Name

Person Who is Reporting Subject Missing:
Address: | Contact Telephone:

Telephone # of investigating agency (accessible 24 hours)
Area Code ( ) -

Authority for Release ☐ Yes ☐ No (Part IV)

Last Seen in Company of: NAME(S)	Sex	Race
(1)		
(2)		

MISCELLANEOUS DATA (Information which may assist in identification: nickname, associates, direction of travel, hairstyle, clothing, etc.)

VEHICLE INFORMATION

License Plate Number	State	Year of Exp.	Lic. Type	VIN

Vehicle Year	Make	Model	Style	Color

Corrective Vision Prescription:

Jewelry Type and Description:

*** MANDATORY DATA ELEMENTS**

PART II

CHECK APPLICABLE CONDITION:

1. ☐ DISABILITY:

   Person missing is under proven physical/mental disability or is senile thereby subjecting herself/himself or others to personal or immediate danger.

2. ☐ ENDANGERED:

   Person missing under circumstances indicating his/her physical safety is in danger.

3. ☐ INVOLUNTARY:

   Person missing under circumstances indicating the disappearance was not voluntary.

4. ☐ CATASTROPHE VICTIM

   Person who missing after a catastrophe.

5. ☐ OTHER

   A person 21 or older, not meeting the criteria for entry in any other category, who is missing and for whom there is a reasonable concern for his/her safety.

PART III

I certify the person described in Part I is missing and that the information I have furnished is true and correct to the best of my knowledge and belief.

Signature	Date	Relationship

PART IV

I authorize any law-enforcement official to use photographs and/or any other identifying information I have provided in any manner they deem necessary in attempting to locate the person I am reporting missing.

Signature	Date	Relationship

Virginia Missing Person Information Clearinghouse
Virginia State Police
Criminal Justice Information Services Division
P. O. Box 27472
Richmond, Virginia 23261-7472

***** IMPORTANT *****

PLEASE ATTACH A CURRENT PHOTOGRAPH OF THE MISSING PERSON TO THIS FORM

314 Checklist for Drug-Endangered Dependent Persons Investigations.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

CHECKLIST FOR DRUG-ENDANGERED DEPENDENT PERSONS INVESTIGATIONS WITH EXPOSURE TO A CLANDESTINE DRUG LAB.

Controlled substances and hazardous materials

- Presence of any illegal or controlled substances or hazardous materials
  - Description of location of any controlled substances or hazardous materials
- Drains and sinks checked for contamination or drainage problems
- Measurements relevant to the reach of a child
- Smells that may indicate fume, chemicals, vapors
- Improperly labeled and incompatible chemicals
- Kitchen surfaces and utensils examined or samples taken (normal cleaning may not remove controlled substances or hazardous materials)
- Presence and location of plastic containers that are indicative of drug manufacture

Living conditions/environment

- Dangerous animals or observations related to animals, such as animal feces and filth
- Inoperable utilities and appliances (gas, electricity)
- Description of beds or sleeping areas
- Available food
- Kitchen and bathroom sanitation
- Unsafe play areas or toys
- Choking hazards
- Fire hazards
  - Combustible materials
  - Inoperable smoke detectors
  - Unsafe heaters
  - Evidence of previous fires

Social factors

- Exposure to pornography or sexual activity
- Whether a child cried or showed emotion when separated from parents
- Social skills and/or peer relations
- Delinquency from school
- Teen pregnancy
- Whether a child exhibited any criminal or violent behavior
- Performance at school

Physical description and health of endangered persons (children or dependent adults)

- Height, weight and reach measurement of each child
- Wounds, punctures, bruises (including bottom of feet)
- Possible chemical burns, particularly to eyes, mouth and nose
- Insect bites
- Known or obvious significant medical conditions, such as cancer, damage to the brain, liver, kidney, spleen, immunologic system, birth defects
- Headache, nausea, dizziness fatigue, shortness of breath or coughing
- Medical exam information, if available
- Indicators of alcohol or drug abuse

314 HIPAA Compliant Medical Records Release Form.pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

HIPAA COMPLIANT AUTHORIZATION FOR THE RELEASE OF PATIENT INFORMATION PURSUANT TO 45 CFR 164.508

TO: _____
Name of Healthcare Provider/Physician/Facility/Medicare Contractor

_____
Street Address

_____
City, State and Zip Code

RE: Patient Name: _____

Date of Birth: _____ Social Security Number: _____

I authorize and request the disclosure of all protected information for the purpose of review and evaluation in connection with a legal claim. I expressly request that the designated record custodian of all covered entities under HIPAA identified above disclose full and complete protected medical information including the following:

☐ All medical records, meaning every page in my record, including but not limited to: office notes, face sheets, history and physical, consultation notes, inpatient, outpatient and emergency room treatment, all clinical charts, r ports, order sheets, progress notes, nurse's notes, social worker records, clinic records, treatment plans, admission records, discharge summaries, requests for and reports of consultations, documents, correspondence, test results, statements, questionnaires/histories, correspondence, photographs, videotapes, telephone messages, and records received by other medical providers.

☐ All physical, occupational and rehab requests, consultations and progress notes.

☐ All disability, Medicaid or Medicare records including claim forms and record of denial of benefits.

☐ All employment, personnel or wage records.

☐ All autopsy, laboratory, histology, cytology, pathology, immunohistochemistry records and specimens; radiology records and films including CT scan, MRI, MRA, EMG, bone scan, myleogram; nerve conduction study, echocardiogram and cardiac catheterization results, videos/CDs/films/reels and reports.

☐ All pharmacy/prescription records including NDC numbers and drug information handouts/monographs.

☐ All billing records including all statements, insurance claim forms, itemized bills, and records of billing to third party payers and payment or denial of benefits for the period _____ to _____.

I understand the information to be released or disclosed may include information relating to sexually transmitted diseases, acquired immunodeficiency syndrome (AIDS), or human

immunodeficiency virus (HIV), and alcohol and drug abuse. I authorize the release or disclosure of this type of information.

This protected health information is disclosed for the following purposes: _____

_____

This authorization is given in compliance with the federal consent requirements for release of alcohol or substance abuse records of 42 CFR 2.31, the restrictions of which have been specifically considered and expressly waived.

You are authorized to release the above records to the following representatives of defendants in the above-entitled matter who have agreed to pay reasonable charges made by you to supply copies of such records:

_____

Name of Representative

_____

Representative Capacity (e.g. attorney, records requestor, agent, etc.)

_____

Street Address

_____

City, State and Zip Code

I understand the following: See CFR §164.508(c)(2)(i-iii)

a. I have a right to revoke this authorization in writing at any time, except to the extent information has been released in reliance upon this authorization.
b. The information released in response to this authorization may be re-disclosed to other parties.
c. My treatment or payment for my treatment cannot be conditioned on the signing of this authorization.

Any facsimile, copy or photocopy of the authorization shall authorize you to release the records requested herein. This authorization shall be in force and effect until two years from date of execution at which time this authorization expires.

_____ _____

Signature of Patient or Legally Authorized Representative Date
(See 45CFR § 164.508(c)(1)(vi))

_____

Name and Relationship of Legally Authorized Representative to Patient
(See 45CFR §164.508(c)(1)(iv))

_____ _____

Witness Signature Date

410 Statewide Standing Order for Nalaxone (1-14-2022).pdf

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

VDH VIRGINIA DEPARTMENT OF HEALTH

Healthy People in Healthy Communities
www.vdh.virginia.gov

Statewide Standing Order for Naloxone

Virginia Department of Health
109 Governor Street, 13th Floor
Richmond, VA 23219

Date Issued: January 14, 2022

The persons identified below are authorized to dispense naloxone pursuant to this standing order and in accordance with protocols developed by the Board of Pharmacy in consultation with the Board of Medicine and the Department of Health. Additionally, this standing order authorizes a licensed pharmacy, wholesale distributor, third party logistics provider or manufacturer to distribute the naloxone formulations specified below via invoice to entities designated by this standing order in accordance with Virginia Board of Pharmacy Guidance Document 110-44.

This order supersedes the orders issued by the State Health Commissioner on April 13, 2018 and March 19, 2020.

Authorized Dispensers:

The following individuals may dispense naloxone pursuant to this standing order to a person to administer to another person believed to be experiencing or about to experience a life-threatening opioid overdose and shall follow Board of Pharmacy protocol when dispensing naloxone as authorized in §54.1-3408 (X) and (Y):

- Pharmacists who maintain a current active license practicing in a pharmacy located in Virginia that maintains a current active pharmacy permit, and
- Emergency medical services personnel as defined in § 32.1-111.1

And the following individuals who have completed a training program in accordance with the policies and procedures of their employer or governing entity:

- Law-enforcement officers as defined in § 9.1-101,
- Employees of the Department of Forensic Science,
- Employees of the Office of the Chief Medical Examiner,
- Employees of the Department of General Services Division of Consolidated Laboratory Services,
- Employees of the Department of Corrections designated as probation and parole officers or as correctional officers as defined in § 53.1-1,
- Employees of regional jails,
- School nurses,
- Other school board employees or individuals contracted by a school board to provide school health services,
- Firefighters,
- Employees of local health departments and contractors or Medical Reserve Corps volunteers acting on behalf of the local health department,
- Employees of local community services boards,
- Persons acting on behalf of a harm reduction site approved by the Department of Health, and
- Individuals acting on behalf of the American Red Cross of Virginia as a Disaster Health Services volunteer.

This order is effective for two (2) years from the date issued, unless otherwise discontinued by the Commissioner or upon his resignation, removal or retirement.

Any individual dispensing naloxone pursuant to this order must maintain a copy of the standing order for two (2) years from the last date of dispensing.

Please call the Office of the Commissioner at (804) 864-7001 with questions about this standing order. Please call the Board of Pharmacy at (804) 367-4456 with questions about the dispensing protocol.

For questions about the REVIVE! training program, please call the Department of Behavioral Health and Developmental Services at (804) 786-0464.

Approved Options for Intranasal or Auto-Injector Administration:

Intranasal	Auto-injector	Intranasal	Intranasal	Injection* (Pharmacists Only)
Naloxone 2mg/2ml prefilled syringe, # 2 syringes Directions: Spray one-half of the syringe into each nostril upon signs of opioid overdose. Call 911. Additional doses may be given every 2 to 3 minutes until emergency medical assistance arrives. **Mucosal Atomization Device (MAD) # 2** Directions: Use as directed for naloxone administration. Must dispense with 2 prefilled syringes and 2 atomizers and instructions for administration.	**Naloxone 2 mg #1 twin pack** Directions: Use one auto-injector upon signs of opioid overdose. Call 911. Additional doses may be given every 2 to 3 minutes until emergency medical assistance arrives.	**Naloxone Nasal Spray 4mg, #1 twin pack** Directions: Administer a single spray intranasally into one nostril. Administer additional doses using a new nasal spray with each dose, if patient does not respond or responds and then relapses into respiratory depression. Call 911. Additional doses may be given every 2 to 3 minutes until emergency medical assistance arrives.	**Naloxone nasal spray 8mg, #1 twin pack** Directions: Administer a single spray intranasally into one nostril upon signs of opioid overdose. Administer additional dose in other nostril using a new nasal spray with each dose, if patient does not respond or responds and then relapses into respiratory depression. Call 911. Additional doses may be given every 2 to 3 minutes until emergency medical assistance arrives.	**Naloxone 0.4mg/ml #2 single-use 1ml vials** Directions: Inject 1ml in shoulder or thigh upon signs of opioid overdose. Call 911. Repeat after 2-3 minutes if no or minimal response. #2 (3ml) syringe with 23-25 gauge 1-1.5 inch IM needles Directions: Use as directed for naloxone administration. Must dispense with 2 single-use 1ml vials, 2 (3ml) syringes and 2 (23-25 gauge) hypodermic needles and instructions for administration.

*** Except for pharmacists, persons authorized to dispense under this standing order shall only dispense formulations for intranasal administration or an auto-injector formulation.**

May refill as long as order remains effective.

Prescriber: Colin M. Greene **Date:** 14 Jan 22

Colin Greene, MD, MPH
NPI Number: 1982693792
Virginia Medical License Number: 0101038830
Virginia Department of Health

INDEX / TOPICS

A

ACKNOWLEDGEMENTS
Discriminatory Harassment. 580
Evidence. 506
Policy manual. 18
Policy revisions. 18
ADMINISTRATIVE INVESTIGATIONS
Criminal parallel. 606
OIS. 73
Vehicle damage. 482
ADMINISTRATIVE LEAVE
Employee convictions. 587
Fitness for duty. 622
Outside employment. 633
ADULT ABUSE. 135
Homeless persons. 365
Investigations. 426
Sexual Assault. 430
AIRCRAFT
Accidents. 327
Flying while armed. 85
Pursuits. 94
Support. 335
ALCOHOL
Firearms. 82
Intoxicants. 170
Vehicle use. 479
AMBER ALERTS. 153
AMMUNITION. 80
ANIMALS
Euthanize. 84
Injured. 84, 404
Service. 217, 234
ANTI-RETALIATION. 584
APPOINTMENTS
ADA coordinator. 213
Chaplain coordinator. 225
Community relations coordinator. 251
fiscal manager. 484
LEP coordinator. 205
Liaison to the homeless community. . . . 364
Operations director. 457, 461
Vehicle maintenance supervisor. 482
Volunteer coordinator. 239
ARRESTS
Biological samples. 222
Child and dependent adult safety. 230
Citations. 312
Diplomatic immunity. 313
Disabled persons. 219
Domestic or family violence. 122
Employee. 587
First amendment assemblies. 378
Homeless persons. 366
Limited English proficiency (LEP). . . . 210
Mass. 376
Mental health. 309
Private Person's. 204
Response team. 278
Safety belts. 609
Towed Vehicles. 406
Warrant service. 457
ASSESSMENTS
Emergency management plan. 26
ASSET FORFEITURE. 435
AUDIO/VIDEO RECORDING
First amendment assemblies. 375
Forced biological samples. 223
OIS. 75
AUDITS
Criminal intelligence system. 340
Informant files. 443
Informant funds. 446
Performance history - quarterly. 655
Personnel complaints. 601
petty cash. 485
Records. 511
AUTHORITY. 11
Abuse of. 364
Command. 22
Ethics. 165
Member. 22
Policy manual. 16
Use of force. 49
AUXILIARY POSITIONS. 191

B

BACKGROUNDS
Ride-alongs. 285
BADGES, PATCHES AND IDENTIFICATION
Administrative leave. 605
Prohibited use. 631
BARRICADE INCIDENTS. 290
BATONS. 57
BIAS-BASED POLICING. 266
BIOLOGICAL SAMPLES. 222
Evidence. 509
Hazards. 328
PREA. 567

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

BODY ARMOR
Suspects. 77
BODY PIERCING. 639
BOMBS
Aircraft accidents. 328
Chaplains. 227
Radios. 297
BRADY. 451
BUSINESS CARDS. 650

C

CANINES
Pursuits. 94, 101
CASH
Asset forfeiture. 435
Audit. 446
Informants. 445
Searches. 558
Vehicle Inventory. 408
CHANGE OF ASSIGNMENT
Tactical team. 279
CHAPLAINS. 224
Ride-alongs. 285
Volunteers. 237
CHIEF EXECUTIVE OFFICER. 14
CHILD AND DEPENDENT ADULT SAFETY 230
CHILDREN
Amber alerts. 153
Child safety. 230
Drug endangered. 133
Firearms. 82
Language assistance. 209, 217
Pursuits. 98
Reports. 179
Transporting. 609
CITATIONS
Accountability. 417
Diplomatic immunity. 314
Jurisdiction. 12
Juvenile. 417
CIVIL
Liability response (OIS). 74
CIVIL COMMITMENTS. 308
Homeless persons. 365
COMMAND STAFF
Anti-retaliation. 585
Claims review. 468
Policy review. 18
PREA reviews. 568
Protocol. 21
Tactical training. 282
Use of force review. 48
Work-related injuries. 636
COMMENDATIONS AND AWARDS
Performance indicators. 656
COMMUNICABLE DISEASES. 594
COMMUNICATIONS FOR PERSONS WITH DISABILITIES. 213
COMMUNITY RELATIONS. 251
COMPENSATORY TIME. 628
COMPUTERS
Digital evidence. 426
CONDUCT
Anti-retaliation. 584
Discriminatory harassment. 140
Fitness for duty. 621
Meritorious. 620
OIS. 69
Personnel complaints. 600
Ride-alongs. 286
Standards of conduct. 169
CONFIDENTIALITY
Adult abuse reports. 139
Chaplains. 228
Communicable disease information. . . 598
Crisis intervention incidents. 306
Fitness for duty. 621
Informants. 441
Performance history audits. 657
Personnel complaints. 602
Protected information. 241
Retaliation complaints. 585
CONFLICT OF INTEREST
Outside employment. 631
CONTACTS AND TEMPORARY DETENTIONS
Bias-based policing. 266
Warrant service. 459
CONTROL DEVICES. 56
Decontamination. 595
COURT ORDERS
Adult abuse. 137
Asset seizure. 436
Biological samples. 223
Child custody. 230
Citation releases. 312
Foreign. 123
Juvenile informants. 441
Marijuana destruction. 509
Members. 587
Property. 508
Source testing. 597
CRIME ANALYSIS. 493
CRIME AND DISASTER SCENE INTEGRITY. 271

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

CRIMINAL INTELLIGENCE SYSTEMS. . 340
CRIMINAL ORGANIZATIONS. 340
CRISIS INTERVENTION INCIDENTS. . . 300
CUSTODIAL INTERROGATIONS
Communications for persons with disabilities. 218
CUSTODIAL SEARCHES. 557
CUSTODIAN OF RECORDS
Personnel records. 615

D

DAILY TRAINING BULLETINS (DTBS)
Training records. 614
DEATH. 179
Chaplains. 227
Custody-Adults. 544
Investigations. 201
Native American Graves (NAGPRA). . 243
Traffic related. 403
DEBRIEFING
Crisis intervention incidents. 306
Warrant service. 459
DECONFLICTION. 463
DEPENDENT ADULTS. 135
Safety. 230
DIPLOMATIC IMMUNITY. 315
DISABLED
Communicating with the. 213
Motorist. 418
DISCIPLINE. 165
Custody-juveniles. 552
Records. 613
Volunteers. 242
DISCLAIMER. 16
DISCRIMINATION
Americans with Disabilities (ADA). . . 213
Limited English proficiency. 205
Personnel complaints. 602
Racial or bias-based profiling. 266
DISCRIMINATORY HARASSMENT. . . 140
Evaluation Form. 580
DOMESTIC OR FAMILY VIOLENCE. . . 120
Member convictions. 587
DRIVING
Pursuit tactics. 93
Safety. 170
Safety belts. 609
Severe use. 474

E

ELECTRONIC MAIL
Personnel complaints. 601
EMERGENCY CUSTODY
Civil Commitment. 308
EMERGENCY OPERATIONS PLAN. . . . 25
EMPLOYEE ASSISTANCE PROGRAM. . 590
ETHICS. 165
EVIDENCE
Bombs. 299
Custodial searches. 557
Digital. 426
NAGPRA. 243
Personnel complaints. 601, 604
Seizing recordings. 359
EXPLOSIONS. 298
EXPOSURE CONTROL
HAZMAT. 287
EYEWITNESS IDENTIFICATION. . . . 339

F

FIREARMS
Civil commitments. 311
Conduct. 170
Destruction of animals. 528
Discharge. 179
Domestic or Family Violence convictions. 587
Off-duty law enforcement actions. . . . 245
Property releases. 507
Pursuits. 97
Retiree concealed. 35
Vehicle maintenance. 474
Vehicle use. 480
FIRST AMENDMENT ASSEMBLIES. . . 374
FISCAL MATTERS. 484
FITNESS FOR DUTY
Medical file. 614
Volunteers. 241
FLYING WHILE ARMED. 85
FOREIGN
Country convictions. 587
Court orders. 123
Currency. 558
Diplomatic and consular representatives. 313
FORMS
Discrimination complaint. 143
Personnel complaints. 601

G

GANGS

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Employee affiliation. 166
PREA. 568
GRIEVANCES
Supervisor authority. 16

H

HANDCUFFING AND RESTRAINTS
Persons with disabilities. 215
HATE CRIMES. 162
HAZARDOUS MATERIAL (HAZMAT) RESPONSE. 287
Aircraft accidents. 328
Handbook. 474
Precautions. 595
Vehicle inventory. 408
HIGH-VISIBILITY VESTS. 398
HOMELESS PERSONS. 364
HOSTAGE AND BARRICADE INCIDENTS
Notifications. 199
Rapid response and deployment. 317
HOSTAGE SITUATIONS. 292

I

IDENTIFICATION CARDS. 650
IDENTITY THEFT
Investigations. 427
IMMUNIZATIONS. 596
IMPAIRED DRIVING. 411
INFORMANTS. 441
INFORMATION TECHNOLOGY. 171
INSPECTIONS
Control devices. 56
Firearms. 82, 85
Personnel. 269
INVESTIGATION AND PROSECUTION. . 424

J

JURISDICTION
Aircraft accidents. 328
Death notifications. 203
Emergency management. 25
Foreign court orders. 123
Identity theft. 427
Multijurisdictional negotiation teams. . . 273
Off-duty law enforcement actions. . . . 246
OIS. 68
Pursuits. 96
Registered offenders. 197
Traffic Accidents. 402

K

KEYS
Searches. 128
Vehicle. 478
KINETIC ENERGY PROJECTILE. 58

L

LACTATION BREAKS. 625
LAW ENFORCEMENT AUTHORITY. . . 11
LIMITED ENGLISH PROFICIENCY. . . . 205

M

MAJOR INCIDENT NOTIFICATION. . . 199
MANDATORY EMPLOYER NOTIFICATION 221
MEAL PERIODS AND BREAKS. 624
MEDIA
Aircraft accidents. 330
First amendment assemblies. 379
Major incidents. 199
OIS. 75
Operations plans. 465
Storage and integrity. 349
Warrant service. 460
MEDICAL
Aircraft accidents. 327
MEDICAL
Barricade situation. 291
Examinations - Adult abuse. 138
Examinations - Child abuse. 133
File. 614
HAZMAT exposure. 287
Homeless persons. 365
Leave Act FMLA. 592
Marijuana. 510
Personnel-body cavity searches. 560
Treatment for OC spray. 58
Treatment for tear gas. 57
Treatment for work-related injury and illness. 635
MEDICAL EXAMINATIONS
Fitness for Duty. 621
MEDICAL FILE. 622

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

MISSING PERSONS
Reports. 179
MOBILE AUDIO/VIDEO (MAV)
OIS. 75
MUTUAL AID
Emergency operations plan activation. . . 25
First amendment assemblies. 377
Warrant service. 459

N

NATIVE AMERICAN GRAVES (NAGPRA) 243
NOTIFICATIONS
Adult abuse. 135
Aircraft accidents. 328
Biological evidence. 509
Bombs. 298
Cash. 485
Custody suicide attempt, death or serious injury. 544
Death. 203
Impaired driving. 413
Impaired Driving. 412
Mandatory employer. 221
Member arrests, convictions and court orders. 587
NAGPRA. 243
OIS. 70
OSHA. 202
Post-OC application. 58
Sick leave. 592
Traffic death. 403
Vehicle towing. 407

O

OATH OF OFFICE. 15
OC SPRAY. 57
OFF-DUTY LAW ENFORCEMENT ACTIONS. 245
OFFICER-INVOLVED SHOOTING (OIS). . 68
Fitness for duty. 622
Notifications. 199
OFFICER SAFETY
Asset forfeiture. 436
Contacts and temporary detentions. . . . 336
Crime and disaster scene integrity. . . . 271
Crisis intervention incidents. 303
Custodial searches. 557
Domestic or family violence. 121
Emergency assistance. 106
Firearm confiscation. 69
Foot pursuits. 101
Informants. 443
Safety belts. 609
Search and seizure. 128
Vehicle pursuits. 88
Vehicle Towing. 409
Warrant service. 457
OPERATIONS PLANNING AND DECONFLICTION. 461
ORGANIZATIONAL STRUCTURE AND RESPONSIBILITY. 21
OUTSIDE AGENCY ASSISTANCE. . . . 195
OUTSIDE EMPLOYMENT. 630
OVERTIME
Limitation on hours worked. 623
Outside. 633

P

PARKING. 479
PATROL. 263
PAYROLL RECORDS
Limitation on hours worked. 623
PEPPER PROJECTILES. 57
PERFORMANCE EVALUATIONS
Sick leave. 593
Volunteers. 239, 241
PERFORMANCE HISTORY AUDITS. . . 655
PERSONNEL COMPLAINTS
Bias-based policing. 267
Brady. 453
Disabled persons. 215, 219
Limited English proficiency. 211
Volunteers. 242
PERSONNEL RECORDS. 613
PHOTOGRAPHS
Aircraft accidents. 329
Field. 338
First amendment assemblies. 375
POLICY MANUAL. 16
PREGNANCY
Custody. 543
PRIVACY EXPECTATIONS
Administrative Searches. 602
Email. 32
Personal communication devices. . . . 470
PRIVATE PERSON'S ARREST. 204
PROTECTED INFORMATION
Ride-alongs. 286
PROTECTIVE CUSTODY
Dependent adults. 137

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

PUBLIC ALERTS. 153
PUBLIC RECORDING OF LAW ENFORCEMENT ACTIVITY. 358
PUBLIC RECORD REQUEST. 516
PURSUITS
Foot. 101
Vehicle. 88

R

RANGEMASTER
Inspections. 79
RAPID RESPONSE AND DEPLOYMENT. 317
RECORDS RELEASE
Adult abuse. 139
Subpoenas and discovery requests. . . . 520
REGISTRANTS. 197
RELIGION
NAGPRA. 243
REPORTING OF ARRESTS, CONVICTIONS AND COURT ORDERS. 587
REPOSSESSIONS. 382
REQUEST FOR CHANGE OF ASSIGNMENT 618
RESPIRATORY PROTECTION. 488
RETIREE CONCEALED FIREARMS. . . . 35
REVIEWS
Anti-retaliation. 586
Chaplain program - annual. 225
Crisis intervention in incidents - annual. . 307
LEP coordinator. 205
Mobile audio/video. 267
Policy manual. 18
Post pursuit. 94, 95
Registrant compliance - annual. 197
Reports. 181
Temporary information files. 341
Use of force review board. 48
Vehicle pursuits - annual. 99
Volunteer program - annual. 239
RIDE-ALONGS. 284
RISK ASSESSMENT. 461

S

SAFETY
Anti-retaliation. 584
Bomb calls. 295
Canine. 478
Conduct. 170
Defective vehicles. 474
Firearms. 81
First responder. 271
Fitness for duty. 621
Hazardous material response. 287
Inspections (vehicle). 474
Shotguns. 77
Unlawful or conflicting orders. 164
SAFETY BELTS. 609
SAFETY EQUIPMENT
Chaplains. 225
First amendment assemblies. 376
Hazardous material response. 289
High-visibility vests. 398
Safety belts. 609
Unmarked vehicles. 475
Volunteers. 238
SEARCHES. 127
Administrative. 605
Body cavity. 560
Custodial. 557
Dead bodies. 202
SEARCH WARRANTS. 457
SICK LEAVE. 592
SOCIAL MEDIA
Media relations. 379
STANDARDS OF CONDUCT. 164
SUBPOENAS
Records release and discovery requests. . 520
SUMMONS
Traffic. 397
SUPERVISION STAFFING LEVELS. . . . 34
SUSPICIOUS ACTIVITY REPORTING. . 384

T

TAKE-HOME VEHICLES. 480
TEAR GAS. 57
TEMPORARY MODIFIED-DUTY ASSIGNMENTS
Outside employment. 633
TOLL LANES. 483
TRAFFIC
Accidents. 402
Citations. 416
Signal malfunctions. 325
Summons. 397
TRAINING
Adult abuse. 139
Bias-based policing. 268
Chaplains. 228
Child and dependent adult safety. . . . 233
Communicable disease. 598
Criminal organizations. 343

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office

Crisis intervention incidents. 307
Custodial searches. 561
Emergency operations plan. 26
Hate or prejudice crimes. 163
Limited English proficiency. 211
Line-of-duty deaths. 671
Negotiation team. 281
Operations planning and deconfliction. . 465
Persons with disabilities. 219, 220
PREA. 570
Pursuits. 100
Rapid response and deployment. 320
Tactical. 280
Volunteers. 240
Warrant service. 460
TRAINING, COMMUNITY RELATIONS. . 254

U

UNIFORMS
Ride-along attire. 285
Volunteer dress code. 238
UNLAWFUL ASSEMBLY. 377
UNMANNED AERIAL SYSTEM. 454
USE OF FORCE
Biological samples. 223
Forced blood samples. 413
Review boards. 48
UTILITY SERVICE EMERGENCIES. . . 325

V

VEHICLE MAINTENANCE. 474
VEHICLES
Inventory. 408
Pursuits. 88
Towing. 406
VOLUNTEERS. 237

W

WARNINGS
Canine. 113
Shots. 85
Traffic. 397
WARRANT SERVICE. 457
WATCH COMMANDERS. 344

Copyright Lexipol, LLC 2023/08/21, All Rights Reserved.
Published with permission by Madison County Sheriff's Office