



# United States Marshals Service **POLICY DIRECTIVES**

## **TACTICAL OPERATIONS**

### **17.4 PEER SUPPORT AND CRITICAL INCIDENT RESPONSE TEAM (CIRT)**

- A. Proponent:** Tactical Operations Division (TOD), Office of Crisis Services (OCS),  
Telephone: 202-307-1555, Fax: 202-307-3446.
- B. Purpose:** This policy directive establishes the United States Marshals Service (USMS) PeerSupport Program (PSP) and provides the policy, guidance and deployment of a Critical Incident Response Team (CIRT).
- C. Authority:** The Director's authority to issue written directives is set forth in [28 U.S.C. § 566](#).
- D. Policy:** The PSP coordinates crisis intervention services and provides USMS employees the opportunity to receive tangible crisis intervention services and stress management education following critical incidents. The PSP will develop and manage a CIRT of volunteer peers who are specially trained and certified in Critical Incident Stress Management (CISM), to be available for immediate deployment in response of critical incidents.
- E. Procedures:**
1. **Critical and Traumatic Incident Situations:** This refers to any event an employee experiences, on or off the job, that is outside the realm of normal human experience and that could produce significant emotional, behavioral or physical reactions. Special support and educational services have been established to deal with potential reactions to critical incident stress situations. CIRT typically partners with the Employee Assistance Program (EAP) on trauma responses. When cases of acute trauma require professional intervention, CIRT will utilize the EAP or contract mental health professionals for referral.
    - a. **Peer Support Program (PSP):** The PSP is designed to provide USMS employees crisis intervention services and stress management education. The PSP will be managed by the Chief Inspector, CIRT, who will serve as the Program Coordinator (PC). Operational control and oversight of the PSP is the responsibility of the Chief, OCS. The PC will develop, manage, and coordinate CIRT, to include:
      - 1) Activation and notification of CIRT to respond to critical incidents;
      - 2) Document relevant statistics of CIRT;
      - 3) Plan and coordinate training and certification requirements for CIRT members;
      - 4) Develop the appropriate recurrent training curriculum and operating procedures for CIRT;
      - 5) Provide training to USMS divisions and departments as needed;

- 6) Serve as an liaison to other agency CISM teams; and
  - 7) Support services for National Police Week.
- b. **Critical Incident Response Team (CIRT):** A CIRT, who has received specialized training in CISM, will respond to critical incidents. The criteria, recruitment, and selection of CIRT members will be the responsibility of CIRT Recruiting & Selection Committee, composed of senior active CIRT members designated by the Chief, OCS. Teams responding to critical incidents will consist of one or more Team members; a Mental Health Professional (MHP) will be available to assist or consult in each of these situations. CIRT will meet with affected employees as soon after the incident as possible, preferably within 72 hours. A Team Leader for CIRT will be designated based on a CIRT call-out schedule and issues surrounding the incident. The Team will attend to the needs of the affected employee(s) and family members. They may not be used to investigate the incident or to supplement the local work force.
- c. **Crisis Management Briefing (CMB):** Whenever there is a Category 1 Critical Incident, a CMB will be conducted by CIRT or by district or division management with the assistance of CIRT. Employees in the affected office must attend. This briefing on the known facts of the critical incident will explain the purpose of the CIRT response and provide a short educational briefing on Critical Incident Stress Management (CISM). A CMB may be conducted following other critical incidents if CIRT or management deems it necessary.
- d. **Critical Incident Stress Debriefing (CISD):** When a CIRT is deployed to a district and CIRT determines that a CISD be conducted, all employees involved in the critical incident must attend. CIRT will also conduct one-on-one debriefings with involved employees as necessary. A CISD is an educational stress debriefing and is not counseling or an operational critique; no notes or records are made of anything that occurs or is said. Depending on the type of critical incident, there may also be a debriefing for the entire affected office, which includes operational and administrative staff.
- e. **Categories of Traumatic Incidents:** The response of CIRT to traumatic incidents will depend on the severity and nature of the incident, the circumstances, and an assessment by management and the Chief, OCS; Chief Inspector, CIRT; or his/her designee:
- 1) Category 1 Incidents: CIRT will automatically respond.
  - 2) Category 2 Incidents: CIRT will respond if the Chief, OCS; Chief Inspector, CIRT; or his/her designee indicate that a response and follow-up is necessary.
  - 3) Category 3 Incidents: CIRT will respond if the Chief, OCS; Chief Inspector, CIRT; or his/her designee indicate that a response and follow-up is necessary or if the district/division management requests assistance.
  - 4) Category 4 Incidents: CIRT can be requested to lead a discussion or meet with employees to reduce stress generated by such

incidents. Telephonic contact will be made to individuals involved in the critical incident, with follow up as necessary.

- 5) **Employee Request:** If CIRT does not respond to a traumatic incident, involved employees may contact CIRT and/or EAP and request services under these programs for themselves and/or their family members.
- 6) **Leave:** The Chief, OCS; Chief, CIRT; or his/her designee in conjunction with district or division management, may grant up to five days of excused absence to employees involved in work-related critical incidents and may request approval of additional leave from HRD, as deemed necessary.

## 2. **Procedures for District Management When Critical Incidents Occur:**

- a. **Reporting Critical Incidents:** The district/division responsible for the individual involved with the significant incident will immediately report it to the USMS Communications Center, as designated in Policy Directive 17.17, [\*Significant Incidents Reporting\*](#). The Communications Center will notify the Chief, OCS; Chief Inspector, CIRT; or his/her designee. Districts/Divisions must prepare a *Report of Significant Incident* within 24 hours of this notification. Any doubts as to reporting incidents of this nature should be resolved in favor of reporting. This policy directive is in no way intended to preclude the normal flow of communications on operational matters.
- b. When an employee is involved in any work-related incident (particularly a shooting) that results in a fatality or serious injury, the employee's supervisor should adhere to Policy Directive 2.1, [\*Shooting Incidents\*](#), Section D.2, to ensure that the appropriate procedures are followed.

## 3. **Deployment of the CIRT:**

- a. **Coordination and Cooperation:**
  - 1) The CIRT direct chain of command is through TOD/OCS, with the Chief, OCS maintaining operational control and oversight. During each deployment the Chief Inspector, CIRT or his/her designee will direct CIRT personnel, logistics and assets.
  - 2) The Chief Inspector, CIRT will have immediate oversight of CIRT activities associated with critical incidents and will coordinate approvals and notifications.
  - 3) Once a Critical Incident has occurred and CIRT has coordinated resources to a district/division, the Chief Inspector, CIRT or his/her designee will contact the appropriate district and/or division management. The Chief Inspector, CIRT or his/her designee will ensure that the United States Marshal (USM), Chief Deputy United States Marshal (CDUSM), appropriate division management, the Assistant Director (AD) and Deputy Assistant Director (DAD), TOD, the Chief, OCS, and the EAP Chief are informed or consulted on significant events.
  - 4) The Chief Inspector, CIRT or his/her designee will coordinate all behavioral health issues with the EAP Chief or his/her designee.

b. **District Support Requirements:**

- 1) Districts must make employees involved in critical incidents available for CIRT support, including CISM activities.
- 2) Districts are required to support CIRT by complying with the availability of selected CIRT deputies to a preplanned operational Team rotation schedule.
- 3) CIRT will set up an operational rotation schedule consistent with unit organization. Team deployment will be based on this schedule, barring exceptional situations. District/Division management will be sent notifications each month of the CIRT call-out schedule.

4. **EAP Referrals and Assessment/Counseling Costs:**

- a. Responding CIRT members will serve as liaisons to employees in need of EAP assistance. CIRT members will provide appropriate educational material, as well as contact numbers for the EAP.
- b. For critical incidents that necessitate referral, EAP will pay for up to six assessment/counseling visits for each affected employee and family member, including the psychological assessment required for employees who experience a life-threatening, work-related critical incident.
- c. Charges for additional visits are the responsibility of the employee and his or her health insurer or the Department of Labor in instances where workers' compensation applies.
- d. See USMS Policy Directive 3.4, [Employee Assistance Program \(EAP\)](#) for additional information and guidance.

5. **Follow-up Services:**

- a. Follow-up services are intended to reduce the stress levels of employees and to assure them of continued USMS support.
- b. Post-traumatic stress follow-up services will be provided to employees and family members through the EAP, as needed.
- c. In consultation and at the direction of EAP, CIRT will conduct mandatory, on-site follow-up visits for districts/divisions in which line-of-duty deaths occur three to six months after such incidents.
- d. Workers' compensation will be provided through the Human Resources Division (HRD), Office of Employee Health Programs. Health benefits claims and all other benefit information will be provided through the HRD, Office of Administrative Staffing and Benefits.
- e. Information on legal considerations will be provided by the Office of General Counsel (OGC).

6. **Affected Family Members:** If the employee wishes, a Mental Health Professional representative or CIRT member will be available to meet with the employee's family. Employees are encouraged to consider this opportunity, since their children, spouses, and parents may also be traumatized by critical incidents.
7. **Confidentiality:** Confidentiality for statements made by the employee will be honored by CIRT in accordance with the EAP confidentiality regulations (unless disclosure is required by other applicable law). Confidentiality may not be honored by CIRT personnel under EAP regulations if CIRT learns of criminal activity, if someone threatens to harm him/herself or others, or if there is a reasonable suspicion that domestic abuse occurred. The sharing of client information between the PSP Coordinator and the EAP Administrator shall not be deemed a disclosure. Under most circumstances, it will not be required to obtain a release from clients to share information between the PSP Coordinator and the EAP Administrator unless applicable law dictates otherwise. This will permit a fluid exchange of information for the purpose of providing appropriate and comprehensive support services.

**F. Responsibilities:**

1. **Assistant Director, TOD:** Formulates policy for and oversees the USMS PSP and CIRT.
2. **Chief, OCS:** Serves as the headquarters point of contact for deployment of the CIRT. Has operational control and oversight of the CIRT and advises the Assistant Director (AD) and Deputy Assistant Director (DAD), TOD, as well as the Office of the Director, on all matters concerning CIRT operations.
3. **Chief Inspector, CIRT:** Immediately, reviews critical incidents and initiates the appropriate responses; advises the Chief, OCS, on all matters concerning operations and deployment of the CIRT. Oversees CIRT activities during operations; ensures that all necessary educational training for CIRT members is provided; monitors and evaluates the CIRT and PSP; maintains necessary records and filing of reports; and adheres to confidentiality requirements.
4. **District/Division Management:** Immediately, informs headquarters when any critical incident occurs, cooperates with CIRT in carrying out their assigned functions, and ensures that deputies assigned to CIRT are available for deployment within 24-hours of critical incidents and available to provide follow-up services on assigned incidents.
5. **Employee Assistance Program Administrator:** Responsible for the coordination of professional behavior health aspects of CIRT responses. Must be kept apprised of all CIRT responses as to ensure that all EAP resources are readily available to impacted employees and family members. An EAP representative, to include the USMS EAP Administrator, or a contracted licensed mental health professional, will always be available for consultation via telephone to the PSP, and will be available to provide intervention and support on-site with the team whenever requested or deemed necessary by the EAP Administrator.

**G. Definitions:**

1. **Critical Incident:** Any event an employee might experience on or off the job, that is outside the realm of normal human experience and that could be expected to produce significant emotional or physical reactions.
2. **Category 1 Incidents:** The following incidents that include:

- a. any incident involving an employee fatality;
  - b. shoot-outs;
  - c. a shooting; suicide or attempted suicide of a fellow worker, witness, etc.;
  - d. an explosion;
  - e. a terrorist attack;
  - f. a hostage situation;
  - g. a plane crash;
  - h. working with dead bodies and/or body parts;
  - i. a catastrophic natural event;
  - j. an employee missing or presumed dead; and
  - k. severe automobile accidents in the line of duty; and violent or traumatic injury to an employee.
3. **Category 2 Incidents:** The following incidents that include major assaults on an employee are:
- a. physical attacks;
  - b. serious death threats;
  - c. being held at gunpoint;
  - d. rescue operations in which a victim dies;
  - e. dealing with and involvement in a hostage-taking or hostage-negotiation situation; and
  - f. suicide or attempted suicide of a prisoner, witness, etc.
4. **Category 3 Incidents:** Incidents that include the following:
- a. violent or traumatic injury to an employee not in the line of duty;
  - b. special operations involving imminent or prolonged danger;
  - c. suicide of a family member;
  - d. involvement in multiple-fatality or infant mortality situations; and
  - e. work-related discharge of weapon at another without injury.
5. **Category 4 Incidents:** Are other traumatic incidents, work related or not, that may cause an employee physical or psychological stress. Supervisors are encouraged to assess the impact of a traumatic incident on an employee or group of employees.

**H. Cancellation Clause:** This policy directive supersedes Policy Directive 17.4, Peer Support and Critical Incident Response Team (CIRT).

**I. Authorization and Date of Approval:**

**By Order of:**

**Effective Date:**

/S/

6-19-2007

John F. Clark

Director

U.S. Marshals Service



## United States Marshals Service POLICY DIRECTIVES

### TACTICAL OPERATIONS DIVISION

#### 17.5 WORKPLACE VIOLENCE PROGRAM

- A. Proponent:** Office of Crisis Services (OCS), Tactical Operations Division (TOD).  
Contact for the HQ Risk Coordinator: Telephone: 202-307-1555, Fax: 202- 307-3446.
- B. Purpose:** This directive establishes the United States Marshals Service (USMS) Workplace Violence Program to address incidents of violence, threats of violence, harassment, intimidation and other disruptive behavior against USMS employees.
- C. Authority:** The Director's authority to direct and supervise all activities of the USMS is set forth in [28 U.S.C. § 561\(g\)](#) and [28 C.F.R. § 0.111](#).
- D. Policy:** The USMS promotes a safe environment for its employees. The USMS is committed to working with its employees to maintain a work environment free from violence, threats of violence, harassment, intimidation, and other disruptive behavior. Violence, threats, harassment, intimidation, and other disruptive behavior in USMS workplaces will not be tolerated.
1. All reports of incidents will be taken seriously and pursued promptly. Individuals who commit such acts may be removed from the premises and may be subject to disciplinary action, criminal penalties, or both.
  2. Such behavior can include oral or written statements, gestures, or expressions that communicate a direct or indirect threat of physical harm.
- E. Procedures:**
1. Any employee who is subjected to, witnesses, or has knowledge of, an act of violence, aggression, or intimidation, or a threat thereof, by another employee (whether on or off the job) and/or experiences or observes such behavior by anyone in the workplace must report the matter to his/her supervisor or to a supervisor in his/her chain of command.
  2. Management, upon learning of an incident, will evaluate the allegations and assess the potential for imminent or future harm. If imminent harm is likely, management will take appropriate action to prevent it. Appropriate action includes, but is not limited to, removing an employee from the worksite, and removing an operational employee's weapon, credentials and GOV. If management deems it necessary to remove someone from the worksite, they should be escorted from the premises by a law enforcement officer. Appropriate action may also include contacting local law enforcement.
  3. Upon intervention in any incident where imminent harm occurred or is considered likely, management will promptly notify his/her chain of command within the branch, division or district and notify the HQ Risk Coordinator, TOD, OCS. Likewise, in situations where management has determined imminent harm is not considered likely but has cause for concern, management is also required to promptly notify his/her chain of command within



the branch, division or district and notify the HQ Risk Coordinator. In either situation, as soon as is practically possible, management will contact the USMS Communications Center and request immediate notification to the HQ Risk Coordinator.

4. The HQ Risk Coordinator will serve as liaison between management and all relevant Headquarters offices, and provide guidance to management and all supporting HQ branches and divisions, until his/her assistance is no longer required. The HQ Risk Coordinator will make all necessary contacts with the appropriate Headquarters offices, including but not limited to the Office of Internal Investigations (OII), Employee and Labor Relations, the Employee Assistance Program, and the Employee Medical Program. The HQ Risk Coordinator acts as a liaison and is not responsible for making the final determination of appropriate action when imminent harm exists.
5. Upon consultation with the appropriate HQ branches and divisions, the employee who perpetrated the incident may be placed on Administrative Leave as determined by management within the branch, division or district, not to exceed 10 days, and may be referred to the Employee Assistance Program (EAP), Office of Internal Investigations (OII), Employee and Labor Relations and/or the Employee Medical Programs.
6. For situations not clearly identified within this policy, the HQ Risk Coordinator can be contacted for assistance in directing management to the proper division and/or services.
7. All information received by the on-site management office, the HQ Risk Coordinator, and the relevant Headquarters office is protected by the Privacy Act, [5 U.S.C. § 552a](#).

**F. Responsibilities:**

1. **All USMS employees:** Every employee is responsible for informing his/her immediate supervisor and/or a supervisor in his/her chain of command of any acts of violence, threats, or actions that could lead to violence in the workplace.
2. **All USMS management:** Every manager is responsible for ensuring, to the extent possible, that a safe and secure work environment exists for employees under his/her supervision. Upon notification of an act of violence or threat of violence and/or action(s) that could lead to violence in the workplace, management is responsible for taking immediate and reasonable steps to attempt to prevent workplace violence. Thereafter, management is required to notify the HQ Risk Coordinator.
3. **HQ Risk Coordinator:** The TOD, OCS has selected a Chief Inspector within the division to serve as the HQ Risk Coordinator. When the HQ Risk Coordinator is notified that an act of violence, aggression, behavior, or intimidation, or a threat thereof, has occurred, the HQ Risk Coordinator is responsible for providing guidance, as needed, but it remains the responsibility of management within the division or district to make the final determination on the course of action to take. The HQ Risk Coordinator serves as liaison between management and all relevant Headquarters offices, coordinating information, services and resources as required between district and/or division management and the relevant Headquarters offices. The HQ Risk Coordinator will serve until his/her assistance is no longer required.
4. **Other Headquarters Offices:** Other Headquarters offices which provide relevant services in the event of incidents of workplace violence include, but are not limited to, the Office of Internal Investigations, Office of the Director, Office of General Counsel, Office of Equal Employment Opportunity, and Human Resources Division. These offices, and

any other Headquarters offices with services relevant to an incident, are responsible for providing guidance and assistance to management and the HQ Risk Coordinator, and for taking whatever independent action is required.

5. **Resources:** Additional guidance is provided on the website of the Office of Personnel Management. [Dealing with Workplace Violence: A Guide for Agency Planners](#).

**G. Authorization Date and Approval:**

**By Order of:**

**Effective Date:**

/S/  
John F. Clark  
Director  
U.S. Marshals Service

7-26-2007



## United States Marshals Service POLICY DIRECTIVES

### TACTICAL OPERATIONS

#### 17.6 SECURITY PROGRAMS MANAGER

- A. Proponent:** Office of Security Programs (OSP), Tactical Operations Division (TOD).  
Telephone: 202-307-5129, Fax: 703-603-7001.
- B. Purpose:** This policy directive provides United States Marshals Service (USMS) policy for the duties of the Security Program Manager (SPM).
- C. Authority:** The Director's authority to direct and supervise all activities of the USMS is set forth in [28 U.S.C. § 561\(g\)](#) and [28 C.F.R. § 0.111](#). Additional authority is derived from [28 U.S.C. § 564](#) and [566](#), [18 U.S.C. § 3053](#) and FRCrP Rule 4(d)(1).
- D. Policy:**
1. In accordance with DOJ [Order 2600.2C](#), the Director of the USMS:
    - a. Will appoint an agency SPM and report this appointment to the Security Programs Staff of the Department of Justice (DOJ);
    - b. May authorize the appointment of additional Headquarters Security Program Officers (HSPO) depending on the size or volume of work in their organization. HSPOs may be required to assist the SPM in the execution of his / her responsibilities and will report to the agency SPM when involved in security program issues; and
    - c. Will authorize field offices to appoint District Security Program Officers (DSPO) to assist in carrying out the organization's security responsibilities in the field. The DSPO will report to the agency SPM when involved in security program issues.
  2. The USMS SPM will be responsible for the following program areas:
    - a. **Personnel Security:** (See Policy Directive 17.7, [Personnel Security](#), for procedures.) Pursuant to Executive Order 10450, ensure that the employment and retention of civilian officers and employees is clearly consistent with the interests of national security (E.O. 10450 as amended, 5 USC 7531 and 5 CFR 731, 732 and 736).
    - b. **Personal Identity Verification:** (Refer to Policy Directive 17.6.2, [Personal Identity Verification](#), for procedures.) Pursuant to Homeland Security Presidential Directive 12, provides for a common identification standard for Federal Employees and contractors.
    - c. **Document Security:** (Refer to Policy Directive 17.6.3, [Document Security](#), for procedures.) Provide for the classification, declassification, and control of national security information and material, including Sensitive Compartmented Information (SCI), pursuant to E.O. 12958, as amended, and granting of USMS employee(s) access to such material. Also provide for the protection of non-

national security information, and information for which safeguarding is required by the Privacy Act of 1974, hereafter referenced as Sensitive But Unclassified (SBU). (E.O. 12958, 5 USC 522a, and Director of Central Intelligence Directive (DCID) 6/4.)

- d. **Physical Security:** (See Policy Directive 17.6.4, [Headquarters Security Procedures](#), for procedures.) Provide for the safety and physical security of personnel and protection of property, which also includes operations security, security education, force protection/antiterrorism, and the security of facilities occupied by the USMS. This program also includes creation and maintenance of Occupant Emergency Plans. (41 CFR 102-74.230, E.O. 12958, 5 USC 522a, National Security Decision Directive (NSDD) 298, 5 USC 301, Presidential Decision Directive (PDD) 39, PDD 62, PDD 63, and DCID 6/9.)
- e. **Communications Security (COMSEC):** (See USMS directive 12.4, [Telecommunications](#) and National Security Telecommunications and Information Systems Policy No. 101 Section 1, b, September 14, 1999, issued by the National Security Agency) Provide USMS oversight and guidance on the management and control of COMSEC devices, keys, equipment, documents, firmware or software embodying or describing cryptographic logic and other items performing COMSEC functions. COMSEC provides measures to deny unauthorized persons information that could be derived from official telecommunications and to ensure authenticity of the communication. Provide for, and monitor, the accounting, use, and access of, classified computer systems and networks to include private networks, standalone work stations, and the JCON-S/TS intelligence network.
- f. **Emergency Planning:** (See USMS National Emergency and Regional Response Plan directives for procedures). Provide for emergency preparedness planning and preparation to enable the USMS to continue its essential operations and discharge its responsibilities during all types of national emergencies, including nuclear or limited war. (E.O. 11490 as amended).

## **E. Responsibilities:**

- 1. **Director, USMS:** Responsible for effective implementation within the organization of the security programs described in this directive and other DOJ orders and directives setting forth specific requirements for these programs.
- 2. **Agency Security Program Manager (SPM):** The SPM is responsible to the Director, USMS, for the management and coordination of all USMS security programs and plans. The agency SPM must maintain a Top Secret, SCI security clearance. Responsibilities of the SPM include, but are not limited to, the following:
  - a. Maintaining coordination and liaison with the DOJ Security Officer and the Department CIO, as appropriate, in the implementation of security programs and in making recommendations for changes of security regulations, policies and procedures;
  - b. Providing that employees are fully informed and periodically reminded of their responsibilities in relation to DOJ security programs. Appropriate training and orientation sessions will be conducted as required. Security Officers and field Security Officers will assist the SPM in training and educational matters;

- c. Observing, enforcing, and when necessary, implementing security regulations or procedures pertaining to the classification, declassification, safeguarding, handling, and storage of classified national security information, SCI, and other DOJ sensitive material;
- d. Establishing and monitoring, as appropriate, DOJ and USMS regulations regarding security of buildings and installations, including control of visitors and maintenance personnel within the area of jurisdiction, and preparing and maintaining an effective Occupant Emergency Plan for Justice occupied buildings as prescribed by General Service Administration (GSA) regulations contained in title 41 CFR;
- e. Ensuring that adequate administrative procedures are established and implemented in the timely evaluation of personnel under E.O. 10450 and Department personnel security regulations. Close coordination must be maintained with the organization's personnel office and with the staff of the DOJ Security Officer in administering these regulations;
- f. Ensuring that adequate physical security controls, administrative procedures, personnel security, and hardware/software security features are implemented in information technology to comply with applicable regulations;
- g. Maintaining coordination and liaison with the DOJ Emergency Coordinator in the review, preparation, and implementation of emergency plans, including vital records matters;
- h. Conducting or arranging for unscheduled inspections of offices and areas during or after working hours to ensure that classified or sensitive information and material is being adequately safeguarded. Problems or deficiencies must be immediately corrected and brought to the attention of the head of the organization;
- i. Where a single DOJ component is not the sole occupant of a building or installation, the SPM of the DOJ component having the largest number of employees in the building or facility will be responsible for ensuring security coordination, including preparation and maintenance of the Occupant Emergency Plan and liaison with GSA regarding guard and physical security matters;
- j. Requiring that all employees having access to classified national security information, including SCI, have the necessary access authorizations, that such authorizations are properly processed, and that their numbers are kept to a minimum. The DOJ Security Officer shall be promptly advised of changes in status wherein an employee's access authorization is no longer required or should be revoked; and
- k. Preparing or maintaining procedures that will provide for a list of combinations on all safes and padlocks employed in their areas of security responsibility and changing of combinations on all safes and locks at least once annually and as prescribed under E.O. 12958, as amended, and [28 C.F.R. § 17](#).
- l. Review of all applications for access to the JCON-S/TS intelligence network by USMS employees and contractors prior to submission to DOJ/JMD/CITP for valid

clearance and justification. Applications submitted to DOJ without an approval memo signed by the SPM (or designee) will be refused.

3. **Headquarters Security Program Officers (HSPO):** HSPOs are responsible to the agency SPM for implementation and administration of security programs as delegated and assigned. HSPOs must maintain a Top Secret security clearance. Their responsibilities include, but are not limited to, the following:
  - a. **Personnel Security**
    - 1) Employee background investigations and reinvestigation;
    - 2) Employment suitability determinations;
    - 3) Employee drug testing;
    - 4) Security clearances; and
    - 5) Related policy, training, and employee briefings.
  - b. **Physical Security and Classified/Sensitive But Unclassified (SBU) Document Security**
    - 1) Electronic security system design, installation, and maintenance;
    - 2) Access control and physical security equipment including keys, locks, and electronic access cards;
    - 3) Control and tracking of classified documents and related audits;
    - 4) Related policy, training, and employee briefings;
    - 5) Top Secret and Secret Document Control Officer;
    - 6) Review all documents or correspondence transmitted or sent outside of the USMS to ensure the documents are properly classified or otherwise designated sensitive. This includes USMS documents sent in response to DOJ/GAO audits;
    - 7) Ensure the disposal and destruction of classified and sensitive material as appropriate; and
    - 8) Prepare and maintain procedures that provide for a list of combinations on all safes and padlocks employed in their areas of security responsibility and changing of combinations on all safes and locks at least once annually and as prescribed under [E.O. 12958](#), as amended, and [28 C.F.R. § 17](#).
4. **District/Division Security Program Officers (DSPO):** DSPOs are responsible to the agency SPM for implementation and administration of security programs as delegated and assigned. DSPOs must maintain a Top Secret security clearance. Each District/Division is required to formally assign this duty utilizing the Form [USM-222](#), *Additional Duty Designation*, and update the employee's M-Wise record to reflect the

assignment. Their responsibilities will be coordinated with the HSPO responsible for each area and include, but are not limited to, the following:

a. Personnel Security

- 1) Maintain list of employees' clearance levels;
- 2) Annual briefing;
- 3) DSPOs will coordinate with the HSPO for Personnel Security on reinvestigations. The HSPO for Personnel Security maintains a centralized database for reinvestigations at headquarters;
- 4) The original SF-312 will be maintained at headquarters in the employee's security file;
- 5) Responsible for outbriefing of personnel leaving the district/division or the USMS and reporting those personnel to the agency SPM. (See Form [USM-199](#), *Separation Checklist*, as prepared by employee's immediate supervisor for pertinent exit procedures.); and
- 6) Responsible for reporting to the HSPO of Personnel Security any individuals from District/Division who are traveling overseas and have an SCI clearance.

b. Classified/SBU Document Security

- 1) Semi - annual review of the clean desk policy;
- 2) Equipment - safes, shredders, secure phones and fax, vaults, courier bags and cards;
- 3) Documents - proper forms are filled out and maintained;
- 4) Access control and physical security equipment including keys, locks and electronic access cards;
- 5) Control and tracking of classified documents and related audits;
- 6) Related policy, training, and employee briefings;
- 7) Top Secret Document Control Officer (TSDCO) & Secret Document Control Officer (SDCO);
- 8) Review all documents or correspondence transmitted or sent outside of the USMS to ensure the documents are properly classified or otherwise designated sensitive. This includes USMS documents sent in response to DOJ/GAO audits;
- 9) Ensure the disposal and destruction of classified and sensitive material as appropriate; and
- 10) Prepare and maintain procedures that provide for a list of combinations

on all safes and padlocks employed in their areas of security responsibility and changing of combinations on all safes and locks at least once annually and as prescribed under [E.O. 12958](#), and as amended in [28 C.F.R § 17](#).

c. Physical Security

- 1) Responsible for ensuring that CSO's are trained in the operation of the screening equipment and producing CSO training logs for DOJ Security and Emergency Planning Staff (SEPS) audits;
  - 2) Responsible for oversight of the status, upkeep and maintenance of the screening equipment and reporting this status during DOJ SEPS audits;
  - 3) Monthly checks of facility security (alarms, cellblock doors and gates, sally port gates, etc);
  - 4) Reports of monthly badge usage;
5. **District/Division OPSEC Coordinator (DOC):** DOCs are responsible to the agency SPM for implementation and administration of the operations security program as delegated and assigned. Their duties and responsibilities are described in the Operations Security Program Standard Operating Procedures (OPSEC SOP) and will be coordinated with the Chief, Operations Security Branch and the District Chief or Division Deputy Assistant Director.

**F. References:**

1. Policy Directive 17.7, [Personnel Security](#)
2. Policy Directive 17.6.2, [Personal Identity Verification](#)
3. Policy Directive 17.6.3, [Document Security](#)
4. Policy Directive 17.6.4, [Headquarters Security Procedures](#)





# United States Marshals Service POLICY DIRECTIVES

## TACTICAL OPERATIONS

### 17.6.2 PERSONAL IDENTITY VERIFICATION (PIV)

- A. Proponent:** Tactical Operations Division (TOD). Telephone: 202-307-9485, Fax: 202-307-9366.
- B. Purpose:** To establish procedures for the identification of United States Marshal Service (USMS) applicants, employees, and contractors for the purpose of authenticating individuals requiring access to federally-controlled facilities and systems in compliance with [Department of Homeland Security \(DHS\) Presidential Directive 12 \(HSPD 12\)](#).
- C. Authority:** The Director's authority to issue written directives is set forth in [28 C.F.R. 0.111](#) and [28 U.S.C. 561\(g\)](#). Additional authorities derived from [HSPD 12](#), signed August 27, 2004, and Department of Commerce, Federal Information Processing Standards (FIPS), [Publication 201, Personal Identity Verification \(PIV\) for Federal Employees and Contractors](#).
- D. Policy:**
1. The USMS verifies and authenticates the identity of each person employed by the USMS in compliance with [HSPD 12](#) prior to issuing an identification card, which provides access to federally-controlled facilities and systems.
  2. Prior to being issued a USMS Federal Employee Identification card and/or receiving access to Department of Justice (DOJ)/USMS systems, all employees and contractors requiring such access receive a background investigation based on the position to be held. At a minimum, this is a Federal Bureau of Investigation (FBI) National Criminal History Check.
  3. All PIV cards are the property of the Federal Government and must be returned at separation or upon request by the USMS Security Program Manager (SPM). All lost or stolen cards are immediately reported to the SPM and the Assistant Chief, Office of Security Programs (OSP), Badge and Credential Program (BCP).
  4. No employee receives access privileges to USMS or DOJ systems until their identity is verified, authenticated, and such request is approved by the USMS PIV Authorizing Official.
- E. Procedures:**
1. **Applicant:**  
Once an applicant to a USMS position (including contractors, task force members, and other government employees) receives a tentative/conditional offer of employment, the identity verification process begins. The following procedures are used to authenticate the identity of the applicant:

- a. The applicant completes the required background investigation questionnaire and forwards it as instructed to the investigating agency.
- b. The applicant reports to the USMS Headquarters or nearest district office to complete Form [USM-394](#), *Personal Identity Verification and Request for Government Identification Card*. The applicant is required to present two forms of identification in compliance with DHS Form [I-9](#), *Employment Eligibility Verification*. This form is signed by the applicant and verifying official. The completed form is sent to one of the following email addresses:

Applicants: [PSB-Applicant@usdoj.gov](mailto:PSB-Applicant@usdoj.gov)

Contractors: [PSB-Contractor@usdoj.gov](mailto:PSB-Contractor@usdoj.gov)

When completing Form [USM-394](#), and prior to forwarding the application package to Personnel Security Branch (PSB)/TOD, the designated applicant or representative ensures all Form [I-9](#) documents are scanned electronically, fingerprints and digital photograph are taken, and all required USMS documentation is completed properly. Applicants going to USMS Headquarters may be sent to a district office for this purpose if necessary. Fingerprint cards are sent to the Assistant Chief, PSB, via official government mail or appropriate mailbox above.

- 1) District Office: The United States Marshal (USM) designates a management-level employee to verify proper completion, sign off, and return Form [USM-394](#). This employee is responsible for the initial identity verification and request for government identification card, taking the applicant's photo/fingerprints, and forwarding them to the Assistant Chief, PSB, via government mail (digital photos may be forwarded on USMS government e-mail only).
  - 2) USMS Headquarters: The Chief, OSP, designates a Personnel Security Specialist to verify proper completion, sign off, and return Form [USM-394](#). This employee is responsible for the initial identity verification and request for government identification card, taking the applicant's photo/fingerprints, and forwarding them to the Assistant Chief, PSB, via government mail (digital photos may be forwarded on USMS government e-mail only). If necessary, the applicant may be referred to the nearest USMS district office to have his/her fingerprints taken. A request is sent by the USM and Chief Deputy United States Marshal (CDUSM) of the selected district.
- c. The Chief, OSP, certifies the identity of the applicant once the required background investigation is completed based on the position. Form [USM- 394](#) is forwarded, along with the Digital Identification (ID) photo of the applicant, to the Assistant Chief, BCP, to have the ID card printed.
  - d. All printed ID cards are forwarded to the USM or Assistant Director (AD) of the employee's assigned district/division as noted on Form [USM 394](#) for issuance. A

copy of Form [USM-394](#) is also forwarded to the AD, Information Technology Division (ITD), or designee. The original Form [USM-394](#) is returned to the Assistant Chief, PSB, and maintained in the appropriate personnel security file (digital photos may be forwarded on USMS government e-mail only).

2. **Contractors: Other than Court Security Officers (CSOs), Special Security Officers (SSOs), and National Physical Security Contractors:**

Contractors requiring full-time unescorted access to USMS space or systems are required to go through a background investigation per USMS Policy Directive 17.6, [Security Programs Manager](#). At the time of the background investigation, the contractor follows the same procedures as noted above for applicants. Contractors who are only employed for a short period of time may be granted escorted access to USMS space in accordance with visitor procedures. Any contractor requiring unescorted access must comply with this policy prior to being given such access.

3. **State and Local Task Force Officers (TFOs):**

State and local TFOs assigned to a USMS district or a Regional Fugitive Task Force requiring full-time unescorted access to USMS space or systems are required to go through a background investigation per USMS Policy Directive 8.14, [Special Deputation Program](#). At the time of the background investigation, the TFO follows the same procedures as noted above for applicants. State and local officers assigned to a Regional Fugitive Task Force may go to the nearest USMS district office to complete the above procedures, in compliance with [HSPD 12](#). TFOs working part-time or less than 6 months may be granted escorted access to USMS space in accordance with visitor procedures. Any state and local TFO requiring unescorted access must comply with this policy prior to being given such access. PIV Cards are not issued to TFOs.

4. **Access to Department of Justice/USMS Information Technology Systems (ITS):**

Once an applicant, contractor, or task force member (including state and local law enforcement) successfully completes a FBI National Criminal History Check and identity verification process, they may request access to USMS ITS. Supervisors are not to submit requests until the background investigations are complete. This request is made via the ITD Form [USM-169](#), *IT User Account Request*, and must be approved by the requestor's supervisor. Once the form is completed, it is forwarded to the AD, ITD, or designee. The AD, ITD, or designee verifies the signed Form [USM-169](#) is received from the Assistant Chief, PSB, before authorizing the applicant's access to information systems and prior to permitting the new employee/contractor to have access to DOJ/USMS information systems.

5. **Issuing or Re-issuing Identity Credentials to Current Employees:**

New background investigations are not required if the results of the most recent background check are on file and can be referenced in the application. Employees submit Form [USM-394](#) as noted in the applicants section above. The Assistant Chief, PSB, signs Form [USM-394](#) verifying that a current favorable background investigation and fingerprints are on file.

- a. The successful completion of all USMS applications and identity verification procedures includes an FBI criminal check and a National Agency Check with Inquiries (NACI). The credential issuing authority notifies the designated applicant representative that the process has been completed and the credential is produced. The credential is delivered to the district office via secure mail.
- b. The applicant appears in person to collect the new credential. Before the credential is issued to the applicant, the USMS-designated credential issuer verifies the identity of the applicant using the following procedure:
  - 1) The individual presents a state or federal government-issued picture identity source document; and
  - 2) The credential issuer validates that the picture and name on the source documents match the information on the new credential.

6. **Revocation of PIV Credentials:**

- a. The revocation process is used to destroy or otherwise invalidate the use of the PIV card. If a USMS employee or contractor separates from the USMS (voluntarily or involuntarily), the PIV card is returned to OSP during the employee exit checkout process.
- b. Lost or stolen PIV credentials must be reported immediately to OSP and Form [USM-169](#) must be completed.

F. **Responsibilities:**

1. **AD/USM/CDUSM:** PIV Requesting Official is responsible for requesting an identity credential on behalf of the applicant.
2. **AD, USM/USMS SPM:** PIV Authorizing Official for individuals who approve the request for an identity credential.
3. **Chief, OSP:** PIV Registration Official is responsible for overseeing identity proofing and background checks. Also is responsible for maintaining identity verification files for all USMS employees and contractors (except CSOs and SSOs).
4. **Chief, Judicial Protective Services:** PIV Registration Official, CSOs, and SSOs are responsible for overseeing identity proofing and background checks. They are also responsible for maintaining identity verification files for all USMS CSOs and SSOs.
5. **Chief, OSP:** PIV Issuing Authority is responsible for overseeing the issuance of identity credentials for the USMS to all employees and/or contractors after all identification proofing, background investigations, and related approvals have been completed.

**G. Cancellation Clause:** This is a new USMS policy directive and remains in effect until superseded.

**H. Authorization and Date of Approval:**

**By Order of:**

**Effective Date:**

          /S/          

          2/2/12          

Stacia A. Hylton  
Director  
U.S. Marshals Service



# United States Marshals Service POLICY DIRECTIVES

## TACTICAL OPERATIONS

### 17.6.3 Document Security

- A. Proponent:** Tactical Operations Division (TOD). Telephone: 202-307-9485, Fax: 202- 307-9366.
- B. Purpose:** This policy establishes the United States Marshals Service's (USMS) procedures for the protection of classified National Security Information, Limited Official Use, Law Enforcement Sensitive, and other unclassified information from unauthorized access. The USMS Security Program Manager (SPM), or designee, is responsible for planning, developing, implementing, and enforcing this policy.
- C. Authority:** Executive Orders [12968](#), [13526](#); the Privacy Act of 1974 ([5 U.S.C. § 552a](#)); Director of Central Intelligence Directive (DCID) 6/4; [32 C.F.R. Part 2001](#), and the Department of Justice (DOJ) [Security Program Operating Manual \(SPOM\)](#).
- D. Policy:**
- 1. Disclosure:** Classified information will be disclosed only to persons with the appropriate security clearance access authorization and a need to know. Classified information will not be disclosed to third party organizations without the permission of the originating component or agency. Unclassified information will be disclosed only to persons whose official duties and responsibilities constitute a need to know.
  - 2. Receipt:** Classified information will be received in a manner which precludes unauthorized access and allows for inspection of possible tampering, the confirmation of contents, and ensures timely acknowledgment of the receipt of Top Secret, Secret, and Confidential information by an authorized recipient.
  - 3. Accountability:** All classified information will be tracked for receipt, distribution, access, reproduction, storing, disposition, and destruction.
  - 4. Reproduction:** Reproduction of classified information will be kept at a minimum, unless otherwise directed by the originating office. Classified information may be reproduced only with the written approval of the SPM.
  - 5. Destruction:** Classified information may be destroyed by burning, shredding, pulping, melting, mutilation, chemical decomposition, and/or pulverizing. Destruction of all classified information is witnessed by the SPM or the Document Control Officer (DCO)/Top Secret Control Officers (TSCO). An additional person, who possesses a security clearance at the same or higher level as the classification of the material that is being destroyed, must also witness the destruction. Unclassified information may be destroyed by any method utilized for classified destruction, but, at a minimum, must be shredded. No documentation or witness to the destruction is required.

## **E. Procedures:**

### **1. Classification of Information:**

- a. An original classification determination specifies the classification level assigned to originally developed source material and establishes the duration of the classification period. The USMS Director is the only person authorized as an Original Classification Authority and the authority may NOT be delegated.
- b. A derivative classification determination specifies the classification level assigned to materials when the sources have already been classified. Derivative Classification Authority is the authority by which other cleared employees of the USMS may extract or summarize information already classified by an Original Classification Authority and specify the same protective markings for classification level and duration of classification. Classification levels are designated as one of three levels:
  1. TOP SECRET: the designation which is applied to information; the unauthorized disclosure of which could reasonably be expected to cause **exceptionally grave damage** to the national security.
  2. SECRET: the designation which is applied to information; the unauthorized disclosure of which could reasonably be expected to cause **serious damage** to the national security.
  3. CONFIDENTIAL: the designation which is applied to information; the unauthorized disclosure of which could reasonably be expected to cause **damage** to the national security.

### **2. Accountability and Tracking Procedures for Classified Documents:**

All Top Secret, Secret, Confidential, and Sensitive Compartmented Information (SCI) documents transmitted to, received by, or otherwise in the custody of USMS offices or personnel are governed by the procedures in this policy. The SPM will establish accountability procedures for all classified documents within the USMS.

- a. A DCO will be appointed (and identified in M-Wise) within the Headquarters Communications Center, Headquarters divisions, and in each district to receive and account for classified documents received and generated by the USMS. Where the DCO and TSCO functions are not performed by the same individual, the DCO will be responsible for controlling and accounting for only those materials classified at the Confidential and Secret levels. The DCO's name and security level should be forwarded to the SPM. The SPM designates an Agency Document Control Officer to coordinate these functions.
- b. A TSCO and Alternate Top Secret Control Officer(s) (ATSCO) are appointed (and identified in M-Wise) within each Headquarters division and district. Their role is to receive, account for, and control all Top Secret documents received and generated by the USMS. Within districts, the function of the TSCO or ATSCO and DCO may be performed by the same individual. The TSCO's name and security level should be forwarded to the SPM. The SPM designates an Agency Document Control Officer to coordinate these functions.

- c. All documents classified as Top Secret, Secret, or Confidential, which are not SCI material, generated or received by any USMS office or employee, will be delivered immediately to either the district DCO/TSCO as appropriate for the classification level or to the Agency DCO/TSCO via divisional DCOs within Headquarters. District DCO/TSCO and the Agency DCO/TSCO assign a control number to documents and prepare Form DOJ-34, *Classified Document Receipt*, for each document. District DCO's register each document in the appropriate Document Control Register prior to transfer to the appropriate recipient. Division DCOs hand-carry the document to the Agency DCO/TSCO for assignment of document control number, preparation of Form DOJ-34, and registering in the appropriate Headquarters Document Control Register. Division DCOs also maintain a division document log into which documents assigned to division personnel are recorded.
- d. All reproduced copies of classified documents are controlled and accounted for in the same manner as the original. All classification and other required markings which appear on the original must also appear on the reproduced copies. Reproduced copies with faint or indistinct markings must be remarked. Certain classified documents may not be reproduced at all. In most cases, this prohibition is clearly marked on the face of such documents. In order to follow the correct procedures, contact the DCO/TSCO or the SPM for assistance.

### 3. **Transmittal Procedures for Classified Information:**

Classified documents are transferred only to persons who have security clearances at least as high as the classification level of the information to which access is required. All classified documents received by the USMS are forwarded to the appropriate recipient without delay by the receiving DCO/TSCO.

- a. Each document received is transmitted with a completed Form DOJ-34. The USMS classified document control number will be noted on the form and on the face of the document. An appropriate classification cover sheet will accompany each document.
  - 1. Classified documents are enclosed within two opaque, sealed envelopes or USMS courier bag. The address of the sender and recipient, completed Form DOJ-34, the overall classification, and any special markings or instructions are placed in the inner envelope.
  - 2. The addresses of the sender and the recipient are placed on the outer envelope.
  - 3. Never place any markings on the outer envelope which would identify the contents as classified information.
- b. Classified information may only be transmitted or discussed over National Security Agency (NSA)-approved cryptographically protected circuits (COMSEC). This includes, but is not limited to: STE, ViPR, SECTERA, SIPR, JCON-S/TS, and JWICS devices and networks.
  - 1. Top Secret information may only be transmitted electronically, as stated above, or hand-carried by an authorized and cleared DOJ messenger service, Defense Courier service, or cleared and designated USMS employees holding valid courier cards. These methods are



acceptable for Top Secret transmission within the United States or between the United States, its Territories, and Canada. *Under no circumstances will Top Secret information be transmitted via the United States Postal Service.*

- c. Secret and Confidential information may be transmitted by any of the methods outlined above for Top Secret, United States Postal Service Express Mail, and by United States Postal Service Registered Mail. All personnel are cautioned to contact the SPM before using the United States Postal Service to transmit Confidential and Secret information if they are unfamiliar with the procedures. The specific requirements vary depending on the destination and certain requirements are also levied on the United States Postal Service.
- d. Transmission of classified information to any foreign government or representative of a foreign government is strictly prohibited unless approval is granted by the SPM. Determinations regarding the release and/or disclosure of classified information must first be made by DOJ in concert with other executive branch agencies.

#### **4. Use and Storage of Classified Information:**

- a. One- and two- drawer security containers which are approved by General Services Administration (GSA) are used primarily in mobile facilities or in areas where small amounts of classified information are stored. Such containers should be securely fastened to floors or located in alarmed or guarded areas to prevent the theft of the container. In addition to security containers meeting GSA standards, Secret and Confidential information may be stored at USMS Headquarters in a non-GSA approved steel filing cabinet equipped with a GSA-approved built-in, three-position, dial-type combination lock, only if the container is located within an alarmed area and specific permission is granted by the SPM.
- b. There will be no external marking identifying the level of classified information authorized to be stored in a container. However, in an area with multiple security containers, each vault, secure area, or security container will be assigned a number or symbol for the purpose of identifying what level or category of classified information is stored therein. The number or symbol will be affixed in a conspicuous location on the outside of the vault or security container.
- c. A record will be maintained by the District/Division Security Programs Officer (DSPO) of the current combination of each vault, secure area, or container used for the storage of classified information. The record will show the location, serial number, date of latest combination change of each such container or vault, manufacturer, and the names and other appropriate identifying data of persons having knowledge of the combinations to such storage facilities. Form [SF-700](#), *Security Container Information*, is used to maintain appropriate information. Form [SF-700](#), containing security combinations will be sealed, marked with the appropriate overall classification (as high as the highest level of information authorized to be stored in the container or vault), and is safeguarded, accounted for, and stored in accordance with the protection afforded to that classification.
- d. The record of the security container combinations as required by item 3 above, must be registered with the DCO/TSCO as appropriate for the level of

classification assigned to the combination. Whenever combinations are changed, the old record of combination will be destroyed. A copy of the classified document receipt or certificate of destruction should be forwarded to the DCO/TSCO as appropriate for the classification level of the combination. The serial number and combination is reported to the SPM.

- e. Combinations to security containers used for the storage of classified information and material will be changed only by individuals having an appropriate security clearance and who have received instruction on how to correctly change such combinations. Combinations will be changed:
  - 1) When the container is initially placed in use.
  - 2) When an individual knowing the combination no longer requires or is authorized access to the classified information stored in the container.
  - 3) When the combination or record of combination has been subject to compromise.
  - 4) Within 1 year of the last combination change.
  - 5) When taken out of service. At this time, built-in combination locks will be reset to the standard combination (b) (7)(E) combination padlocks will be reset to the standard combination (b) (7)(E)
- f. Form [SF-702](#), *Security Container Check Sheet*, is conspicuously affixed to the outside of all security containers used for the storage of classified information to identify those persons having opened or closed the containers.
  - 1) Each authorized person records the time and date that he/she unlocks or locks the security container, followed by the person's initials.
  - 2) At the close of each working day, a person other than the individual locking the container checks the container, in the presence of the individual locking the container, to ensure that it is secure. The time of the check, followed by the checker's initials, is recorded. The check is conducted each working day.
  - 3) If a container has not been opened, the date, time, checker's initials, and the notation "Not Opened" are entered.
- g. A container is not to be left unattended until it has been locked by an authorized person and checked by a second person. The person locking a container is responsible for ensuring that another person checks the container.
- h. Reversible "Open-Closed" signs are placed on security containers containing classified information. The respective side of the sign is displayed to indicate when the container is open or closed. Other security signs are placed on containers as directed by the SPM.
- i. Classified documents, when removed from storage for working purposes, are kept under constant surveillance and turned face-down or covered when persons who are not authorized access to the information are in the area. Form [SF-703](#), *Top Secret*; Form [SF-704](#), *Secret*; or [Form SF-705](#), *Confidential*, cover sheets should be utilized to cover classified documents.

- j. Preliminary drafts, carbon sheets, computer media, plates, stencils, stenographic notes, worksheets, and all similar items containing classified information will be either destroyed by the person responsible for their preparation immediately after they have served their purposes, or is given the same classification and safeguarded in the same manner as the classified information they contain.
- k. **Clean Desk Policy:** USMS managers, in conjunction with DSPO, ensures a system of security checks is implemented at the close of each working day to ensure that classified information is properly protected. USMS managers will require the custodians of classified information to conduct an inspection at the end of each working day to ensure:
  - 1) All classified information, including computer media such as floppy disks, CDs, and DVDs used during classified processing sessions, is stored in approved security containers;
  - 2) Waste material in burn bags, if utilized, are either stored in approved security containers or destroyed;
  - 3) Classified shorthand notes, carbon paper, carbon and plastic typewriter ribbons, rough drafts, and similar papers have been properly stored and/or destroyed; and
  - 4) Each security container used to store classified information is checked to ensure it is properly secured.

5. **Law Enforcement Sensitive (LES):**

- a. LES information used by the USMS must be maintained, distributed, secured, and disposed of in a manner that will protect the information against unauthorized disclosure. LES information is unclassified information of a sensitive and proprietary nature that if disclosed could cause harm to law enforcement activities by jeopardizing investigations, compromising operations, or causing life threatening situations for confidential informants, witnesses, or law enforcement personnel. This information must be protected against release to unauthorized individuals. This term is prescribed for use within DOJ and the USMS to signify and identify such information.
- b. The following categories of information are designated as LES information and must be marked accordingly:
  - 1. Informant and Witness information;
  - 2. Grand Jury information subject to the [Federal Rules of Criminal Procedure, Rule 6\(e\), Grand Jury Secrecy of Proceedings and Disclosure](#);
  - 3. Investigative material;
  - 4. Law enforcement sources and undercover operations;
  - 5. Law enforcement intelligence sources and methods;
  - 6. Federal law enforcement agency activities;

7. Federal support to state/local law enforcement activities;
8. Joint federal, state, and local law enforcement activities;
9. Information pertaining to the judiciary, to include investigations of inappropriate communications; and
10. Personnel information pertaining to employees of the USMS.

**6. Limited Official Use (LOU):**

- a. LOU information used by the USMS must be maintained, distributed, secured, and disposed of in a manner that will protect the information against unauthorized disclosure. LOU information is unclassified information of a sensitive, proprietary, or personally private nature which must be protected against release to unauthorized individuals. This term is prescribed for use within DOJ and USMS to signify and identify such information.
- b. The following categories of information are designated as LOU information and must be marked accordingly:
  1. Tax information subject to [26 U.S.C. § 6103](#), *Confidentiality and Disclosure of Returns and Return Information*, as to persons filing income tax returns;
  2. Information that could be sold for profit;
  3. Personal information subject to [5 U.S.C. § 552a](#), *Privacy Act of 1974*;
  4. Memoranda or reports that disclose security vulnerabilities;
  5. Information that could result in physical risk to individuals;
  6. Company proprietary information;
  7. Audit staff work papers;
  8. Draft audit reports;
  9. Information offered in confidence during the conduct of internal audits, comprehensive assessments, program reviews, and evaluations;
  10. Program and budget information on intelligence-related activities; and
  11. Sensitive material subject to The Antideficiency Act.

**7. Procedures for LES and LOU Information:**

- a. The USMS Director is authorized to determine which categories of information, in addition to the above, should be designated as LOU and which categories are of such sensitivity that they may require protective measures.

- b. Unclassified information that has been determined to require protection against unauthorized disclosure must be identified as LOU to ensure that all persons having access to the information are aware of the protection requirement. The preferred method of identification of LOU material is to mark "LIMITED OFFICIAL USE" on the first page of the material. Material containing LOU information may further be identified by the use of Form [USM-5, Limited Official Use Cover Sheet](#). The use of this cover sheet is primarily to protect against inadvertent visual disclosure of information on the first page. It may be used in lieu of the requirement to apply the LOU marking to the first page of the material. When cover sheets are so used, they should be affixed to documents using staples rather than paperclips, so as to preclude disassociation of the document from the cover sheet. Large or otherwise voluminous quantities of unmarked LOU information housed in a protected area or in containers within a protected area need not be individually marked until the information is removed from the storage container or protected area. Protected areas or containers storing information designated as LOU, but not yet individually marked, must themselves be posted to identify the contents as LOU and to promulgate the requirement to mark individual records when they are removed from the container for any reason.
- c. Personnel who have custody of material designated as LOU must exercise due caution to ensure that the information is not available to individuals who do not have a need to know. At a minimum, unauthorized individuals must not be able to enter areas unobserved and gain visual access to LOU information.
- d. During non-duty hours, LOU material is locked in a desk or file cabinet, or stored in a facility or area with adequate physical access control measures to prevent unauthorized access. A safe or file cabinet, protected with a GSA-approved combination lock, is recommended for higher-sensitivity LOU material.
- e. LOU information stored and processed by computer systems will have adequate physical, administrative, and technical safeguards as described in Policy Directive 12.7, [Information Technology \(IT\) Security](#).
- f. Grand Jury information, when not in use, at a minimum, is stored in a file cabinet equipped with a locking bar and locked with a GSA-approved dial-type, three-position, changeable combination padlock. Access to combinations protecting Grand Jury information will be limited to those having a need to know, and will be changed under the same conditions as combinations protecting classified information. Additional security measures may be required at the discretion of the cognizant United States Attorney if it is determined by the United States Attorney to be warranted.
- g. Information which has been identified and is known by the recipient as LOU will be safeguarded from disclosure to unauthorized individuals whether or not the material is physically marked. Safeguarding from disclosure includes precautions against oral disclosure, prevention of visual access to the information, and precautions against release of the material to unauthorized personnel.
- h. LOU information leaving the control of the USMS must be transmitted in a single opaque envelope or wrapping properly sealed and addressed. The envelope or wrapping will not be marked "LIMITED OFFICIAL USE" or "LOU." Grand Jury information which cannot be personally transmitted between authorized recipients will be sent by United States Postal Service Certified Mail with return receipt.

- i. Electronically transmitted messages or data containing LOU information will be preceded by the term "Limited Official Use" at the beginning of the text.
- j. LOU information may be discussed on the telephone; however, the ease of interception of telephone conversations dictates that discretion be used where the threat of interception exists. In this case, the use of secure telephones should be considered.
- k. If LOU information must be released to non-government personnel as part of a contract or grant, those personnel must have a favorably adjudicated background investigation of the same scope as is required for USMS employees, prior to granting access to LOU information.
- l. LOU information should be destroyed by shredding, burning, pulping, mutilation, and/or any means that would preclude reconstruction of the material. LOU information of the highest sensitivity should be destroyed, when possible, in a manner similar to that used for classified information.
- m. Microfiche and microfilm should only be destroyed by burning or melting. Do not shred or pulverize, as small particles of this material can contain large amounts of readable LOU information.
- n. Computer storage media containing LOU information will be overwritten or degaussed prior to release of the storage media outside the USMS. Contact the Computer Security Officer for specifics regarding software and procedures for affecting such data overwrite.
- o. The safeguards prescribed herein for safeguarding LOU information are the minimum requirements except where noted. The sensitivity of this information, nature or extent of the threat of unauthorized access, and the potential damage resulting from unauthorized access must be considered in determining the adequacy of existing safeguards and the need for additional security protection.

**8. Destruction of Information:**

- a. Classified material may be destroyed by burning, shredding, pulping, melting, mutilation, chemical decomposition, or pulverizing (hammer mills, choppers, and hybridized disintegration equipment). Pulpers, pulverizers, or shredders may be used only for the destruction of paper products. High wet strength paper, paper mylar, durable-medium paper substitute, or similar water repellant type papers are not sufficiently destroyed by pulping; other methods such as disintegration, shredding, or burning will be used to destroy these types of papers. Classified material in microform (microfilm, microfiche, or similar high data density material) may be destroyed by burning or chemical decomposition, or other methods approved by the SPM.
- b. Top Secret, Secret, and Confidential classified information and material (record and non-record) will be destroyed in the presence of an appropriately cleared official by burning, melting, chemical decomposition, pulping, pulverizing, shredding, or other mutilation sufficient to preclude recognition or reconstruction of the classified information.
- c. Shredder machines must meet NSA standards for destruction of material

of that classification level.

- d. Classified information identified for destruction will be destroyed completely. Residue is inspected during each destruction, to ensure that classified information cannot be reconstructed.
- e. Specific instructions for destruction of classified computer media and components may be found in the [SPOM – Annex G](#).
- f. Form DOJ-34 will be completed for each document being destroyed to attest to the destruction of Top Secret, Secret, and Confidential documents. Form DOJ-34 is forwarded to the DCO/TSCO as appropriate and will contain the date, time and place of destruction, identification of the document(s) destroyed, the reason for destruction, the method of destruction, and the name and signature of the official and the witness destroying the material. If destruction is accomplished by an approved central disposal system, the destruction certificate will be signed by the witnessing officials at the time the material is delivered at the facility. USMS Headquarters personnel should ensure that a copy of the completed DOJ-34 is also provided to the DCO. Certificates of destruction are maintained by the DCO/TSCO for a minimum of 2 years, after which they may be destroyed.
- g. Unclassified material may be destroyed by any method used for destruction of classified information. At a minimum, it must be shredded. The destruction of unclassified material does not have to be documented or witnessed.
- h. The use of private company “document destruction services” may be appropriate in certain circumstances, but their use must be approved by the SPM and may be subject to additional procedural requirements.

9. **Security of Meetings and Conferences:**

- a. The USMS official responsible for arranging or convening a meeting where classified information will be disclosed is also responsible for instituting procedures and selecting facilities which provide adequate security. The SPM provides information on secure areas that may be used for classified meetings.
- b. Meetings during which classified information is to be discussed will be held only in a United States Government facility or at a cleared facility of a USMS contractor or consultant. When necessary for the accomplishment of essential functions, a meeting involving classified information may be held at another location provided it has been authorized by the SPM.
- c. The USMS official responsible for hosting the meeting or conference will notify each person present of any security limitations that must be imposed because of the level of access authorizations of the attendees or the physical security conditions of the facility. Additionally, the USMS official responsible for the meeting will:
  - 1. Ensure each person attending the classified portions of the meeting has been authorized access to information of equal or higher classification than the information to be disclosed;
  - 2. Ensure the area in which classified information is to be discussed



affords adequate acoustical security against unauthorized disclosure;

3. Ensure that adequate storage facilities are available, if needed;
4. Control and safeguard any classified information furnished to those in attendance and retrieve the material or obtain receipts, as required; and
5. Monitor the meetings to ensure that discussions are limited to the level authorized.

**10. Classified Information Security Violations:**

- a. Any person who suspects or has knowledge of a security violation pursuant to this policy, including the known or suspected loss or compromise of National Security Information (NSI), will promptly report telephonically and confirm in writing the circumstances to the SPM.
- b. Sanctions include, but are not limited to, warning notices; disciplinary action; suspension or termination of security clearance; and as permitted by law, suspension without pay; forfeiture of pay; removal or dismissal; and prosecution.
- c. Sanctions will be imposed upon any person subject to these regulations and responsible for a violation specified under this policy as determined by the USMS Director or the United States Attorney General.
- d. USMS employees are subject to appropriate administrative and criminal sanctions if they:
  1. Knowingly and willfully improperly classify or continue improper classification of information.
  2. Knowingly, willfully, and without authorization disclose classified information or compromise classified information through negligence.
  3. Knowingly and willfully violate any other provision of [28 C.F.R. § 17](#), *Classified National Security Information and Access to Classified Information*, or this policy.

**F. Responsibilities:**

**1. SPM:**

- a. Developing and administering procedures and policies pertaining to the receipt, generation, handling, safeguarding, storage, and disposal of all classified material and information within the USMS;
- b. Compiling and maintaining classified document accountability records for all classified material generated or received by the USMS. This is accomplished through inventory reporting from DSOs and auditing;
- c. Providing technical assistance to USMS Headquarters and district offices; and
- d. Maintaining coordination and liaison with the DOJ Security Officer in the



implementation of USMS policy and procedures.

2. **DSO:** Every district and division office designates a person to perform the duties of a DSO. The DSO is responsible for the receipt, recording, accountability, and destruction of all Secret and Confidential classified documents coming into their offices. USMS Headquarters DSOs are also responsible for taking classified documents to the Agency DSO for recording and accountability and that all document transfers and destruction actions are properly documented and recorded.
3. **USMS District/Division Top Secret Security Officer (TDSO):** The TDSO in every district and division will be designated to perform the duties of the TDSO. They are responsible for the receipt, recording, accountability, and destruction of all Top Secret classified documents coming into division/district offices. USMS Headquarters TDSO's will coordinate with the Agency TDSO to track and destroy classified documents. TDSOs exercises controls over Top Secret information within the district.

**G. Definitions:**

1. **Original Classification Authority:** The authority delegated by the United States Attorney General to the USMS Director to make initial determinations as to whether information requires a certain degree of protection against unauthorized disclosure in the interest of national security. An original classification determination specifies the classification level assigned to the information and the duration of that classification.
2. **Derivative Classification Authority:** The authority by which employees of the USMS may extract or summarize information already classified by an Original Classification Authority and specify the same protective markings for classification level and duration of classification.
3. **Classified Information:** Also known as NSI, it is information (in any form or medium) or material that is owned by, produced for or by, or under the control of the United States Government and determined under security Executive Orders and this policy to require protection against unauthorized disclosure.
4. **Top Secret:** The designation which is applied to information, the unauthorized disclosure of which could reasonably be expected to cause **exceptionally grave damage** to the national security.
5. **Secret:** The designation which is applied to information, the unauthorized disclosure of which could reasonably be expected to cause **serious damage** to the national security.
6. **Confidential:** The designation which is applied to information, the unauthorized disclosure of which could reasonably be expected to cause **damage** to the national security.
7. **Compromise:** The disclosure of classified information to persons not authorized thereto or without a need to know. **The failure to properly secure classified information in accordance with this section is considered a compromise.**
8. **Custodian:** An individual who has possession of, or is otherwise charged with the responsibility for safeguarding or accounting for classified information as designated by the USMS Director.

9. **Document:** Any recorded information, regardless of its physical form or characteristics. Examples include, without limitation:
- a. Written or printed matter;
  - b. Data processing cards and tapes;
  - c. Maps;
  - d. Charts;
  - e. Paintings;
  - f. Drawings, engravings, and sketches;
  - g. Working notes and papers;
  - h. Reproductions by any means or process; and
  - i. Sound, voice, magnetic or electronic recordings in any form.
10. **Foreign Government Information:** Information that is:
- a. Provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both are to be held in confidence.
  - b. Produced by the United States pursuant to, or as a result of, a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.
11. **Information:** Knowledge that can be communicated by any means.
12. **Information Security:** The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by Executive Order, DOJ Order, or statute.
13. **Intelligence Activity:** An activity that an agency within the intelligence community is authorized to conduct under [E.O. 12333](#), *United States intelligence activities*.
14. **Material:** Any product or substance on, or in which, information is embodied.
15. **National Security:** The national defense and foreign relations of the United States.
16. **SCI:** Information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentalization is established.
17. **Unauthorized Disclosure:** A communication or physical transfer of classified information to an unauthorized recipient.

18. **Unclassified Information:** Any information that may contain references, either direct or indirect, to USMS business, personnel, operations, facilities, capabilities, organization structure, or activity that has not been designated as Classified Information.

H. **References:** None.

I. **Cancellation Clause:** This policy directive supersedes Attachment C, *Document Security*, Policy Directive 17.6, *Security Programs Manager*.

J. **Authorization and Date of Approval:**

By Order of:

Effective Date:

          /S/            
Stacia A. Hylton  
Director  
U.S. Marshals Service

          August 13, 2012



# United States Marshals Service POLICY DIRECTIVES

## TACTICAL OPERATIONS

### 17.6.4 HEADQUARTERS SECURITY PROCEDURES

- A. Proponent:** Office of Security Programs (OSP), Tactical Operations Division (TOD).  
Telephone: 202-307-9427, Fax: 202-307-9366.
- B. Purpose:** The purpose of this policy directive is to establish policy and procedures for the safe and secure operation of the United States Marshals Service (USMS) Headquarters.
- C. Authority:** The Director's authority to supervise the USMS and issue written directives is set forth in [28 C.F.R. § 0.111](#) and [28 U.S.C. § 561\(g\)](#). The authority to establish safety procedures is derived from Department of Justice (DOJ) Order 2600.2D, [Security Programs and Responsibilities](#).
- D. Policy:**
1. Under no circumstances should security procedures, capabilities of screening equipment, post assignments, manpower, or any other information relating to the USMS or the security of any person, place, or mission be discussed with anyone who is not a USMS employee or Special Security Officer, nor should any information be discussed within the hearing of any member of the general public or other person who has not been designated as having a need to know by the Assistant Director (AD), TOD, or his/her designee. Any disclosure of the information contained herein, whether intentional or inadvertent, must be reported in writing to the AD, TOD, through the Chief Inspector for Headquarters Security, OSP, within 1 hour of the disclosure or the discovery that the information has been disclosed.
  2. Security Contractors:
    - a. In order to provide security to USMS Headquarters, Security Contractors are employed for the purposes of access control, screening, and emergency response.
    - b. Security Contractors may not accept changes to their orders from any person outside of their chain of command.
    - c. Security Contractors are to be used for access control and security response only. They should not be requested to perform additional duties, such as answering telephones or serving as a receptionist.
    - d. USMS employees, contractors, and visitors are required to obey all commands issued by Security Contractors or other USMS employees who are responsible for the security of USMS Headquarters.
  3. Access Control:
    - a. The following personnel are permitted unescorted access to USMS Headquarters facilities:

- 1) USMS Employees
- 2) USMS Contractors (with OSP approval)
- 3) DOJ Employees (with issued credentials)
- 4) Administrative Office of the United States Courts Employees
  - a) Who must regularly visit USMS Headquarters
  - b) Who have a building identification card
- b. Requests for unescorted access must be made by a USMS employee at the grade of Assistant Chief (GS-14) or higher.
- c. All USMS employees, contractors, interns, and temporary duty employees have 24-hour access to Headquarters.
- d. Non-USMS Controlled Access Points:
  - 1) Certain doors and parking garage gates are controlled by the building management company, not by the USMS.
  - 2) Access devices such as proximity cards or key fobs to open these areas are issued by the Office of Facilities and Courthouse Construction (OFCC), Management Support Division.
  - 3) Loss of these devices must be reported to OFCC in accordance with their established policy and procedures.
  - 4) Possession of an OFCC-issued access control device does not indicate that a person is permitted access to USMS-controlled space or buildings.
4. Weapons:
  - a. USMS operational personnel otherwise authorized to carry their weapon pursuant to Policy Directive 2.3, *Firearms*, are permitted to carry their firearms in USMS Headquarters.
  - b. (b) (7)(E) [REDACTED]
  - c. (b) (7)(E) [REDACTED]
  - d. (b) (7)(E) [REDACTED]
  - e. (b) (7)(E) [REDACTED]

- f. Weapons are as defined in [18 U.S.C. § 930](#) and include, but are not limited to, firearms, knives, clubs, batons, electronic control devices, projectile stun guns, and chemical weapons.
  - g. Small pocket knives (with a blade that is less than 2.5 inches) may be carried.
  - h. Persons without proper authorization who attempt to bring a weapon into USMS-controlled space may be prosecuted.
- 5. Requests for unescorted access other than those specifically outlined in this policy must be submitted in writing to the Security Program Manager (SPM).
  - 6. Requests must include a justification as to why the individual requires unescorted access to USMS Headquarters.
  - 7. Requests must be made by a USMS employee in the grade of Assistant Chief (GS-14) or higher.
  - 8. The SPM will be the deciding official for unescorted access.

**E. Responsibilities:**

- 1. All Special Security Officers, Lead Special Security Officers, and the Site Supervisor are responsible for reading, learning, and understanding the policies and procedures contained herein. Employees, contractors, and visitors are responsible for obeying all security requirements set forth under this policy. All personnel will obey the security instructions given by the SPM, Chief Inspector for Headquarters Security, and the Security Contractor.
- 2. **SPM:** The Chief, OSP, is designated as the SPM for the USMS and is responsible for personnel security, personnel identity verification, physical security, emergency planning, and communications security. The SPM is designated as the responsible official for all matters relating to the security of USMS Headquarters.
- 3. **OFCC:** Responsible for physical security equipment in the USMS Headquarters complex which includes, but is not limited to, cameras, monitors, alarms, card readers, door releases, and other physical security equipment.
  - a. OFCC will maintain the National Repair Contract for USMS space.
  - b. OFCC will provide two representatives to the Facility Security Committee; one will represent physical matters and one will represent OFCC on issues pertaining to the building and leases.
- 4. The Chief Inspector for Headquarters Security serves as the Contracting Officer's Representative (COR) for the security officer contracts and will serve as the primary program manager for all matters pertaining to securing USMS Headquarters buildings. The Chief Inspector for Headquarters Security will consult with OFCC on all physical security improvements to USMS Headquarters.
- 5. ADs are responsible for ensuring personnel under their supervision comply with all requirements in this policy directive.

## F. Procedures:

1. Building Identification Cards (BIDs):
  - a. All personnel in USMS-controlled space must wear their identification cards. Permanently assigned personnel will be issued BIDs by OSP. A BID will bear the person's photo, last name, and expiration date. At the SPM's designation, the identification card may contain a colored background to indicate employment status.
  - b. BIDs must be worn between the shoulder and the waist, and be clearly visible at all times. BIDs will be shown to security personnel to gain entry into USMS-controlled space. It must also be shown on demand whenever requested by any USMS employee.
  - c. BIDs issued to USMS employees are valid for 5 years from the last day of the month of issue.
  - d. BIDs issued to non-USMS employees are valid for 1 year from the last day of the month of issue.
  - e. Requests for a BID will be processed using Form [USM-394, Personal Identity Verification \(PIV\)/ Building Access Card Request](#). This will be completed in accordance with the instructions on the form.
  - f. BIDs will only be issued to personnel who have a current compliant [Homeland Security Presidential Directive \(HSPD\)-12](#) background investigation on file.
  - g. Only USMS employees may sign as a supervisor on Form [USM-394](#). Digital signatures are required.
  - h. Renewal notices will be sent out by e-mail approximately 1 month prior to the expiration date on the BID.
  - i. A new Form [USM-394](#) must be completed and signed by the USMS supervisor and sent to TOD.
  - j. Lost badges will be reported immediately by e-mail to the Chief Inspector for Headquarters Security. Replacement badges will be issued when the Form [USM-394](#) is received by TOD. Repeated loss of a BID by an individual may result in referral for disciplinary action or denial of a new BID.
  - k. For renewals or lost BIDs, the TOD employee making the badge will verify the status of the requestor in M-Wise prior to creating the new BID. All questions will be referred to the Assistant Chief, Document Security and Badges Branch.
  - l. Employees or contractors who have lost or misplaced their BID may be issued Form [USM-567, Employee Building Pass](#), as temporary identification upon the

presentation of their USMS-issued credentials to the security contractor in the lobby of 1750 Crystal Drive. If they do not have USMS-issued credentials, then a USMS employee must come to the security contractor station in the lobby of 1750 Crystal Drive and vouch for the employee or contractor. Form [USM-567](#) is used as temporary identification of USMS employees or contractors and is not valid unless a valid government photo identification card is presented with it.

- m. For temporarily misplaced BIDs, Form [USM-567](#) will be issued in lieu of a new BID.
  - n. Expired BIDs are invalid. Expired BIDs will not be permitted to be used as identification to enter USMS-controlled space. Invalid BIDs will be seized by the security contractor.
  - o. BIDs remain the property of the USMS at all times and must be returned upon termination of employment or expiration.
  - p. BIDs may not be shared for any reason. BIDs in the possession of any person other than the individual it was issued to will be seized by the security contractor.
  - q. Personnel may only possess one USMS Headquarters BID at a time.
  - r. BIDs will be obscured from public view when USMS employees or contractors are outside of a USMS-controlled space.
  - s. BIDs will not be displayed in automobiles by hanging them from the rear view mirror, placing them on the dashboard, or leaving them in public view.
  - t. USMS employees and contractors should consider covering USMS badges, seals, and other insignia when outside USMS-controlled space.
2. Temporary visitors will be issued single-use paper badges which must be returned upon departure.
3. Requests for unescorted access other than those specifically outlined in this standard operating procedure must be submitted in writing to the SPM.
- a. Requests must include a justification as to why the individual requires unescorted access to USMS Headquarters.
  - b. Requests must be made by a USMS employee in the grade of Assistant Chief (GS-14) or higher.
  - c. The SPM will be the deciding official for unescorted access.
4. Security Screening:
- a. All security screening for personnel will be conducted at 1750 Crystal Drive.
    - 1) All visitors must be screened before being issued temporary identification or being permitted to leave the Security Contractor Station with their escorts.
    - 2) USMS employees or contractors with a BID are exempt from routine screening. If required by the security situation, this exemption may be revoked.



- 3) Screening policy and procedures are specified in the Security Contractor post orders.
  - b. All mail and packages will be screened at the USMS Warehouse.
    - 1) Mail and package screening procedures will be specified in the Security Contractor post orders.
    - 2) Mail and packages will not be accepted anywhere other than the USMS warehouse.
    - 3) Couriers from other federal agencies will be permitted to make deliveries to USMS-controlled space.
5. Escort:
- a. All persons issued Form [USM-567](#), *Employee Building Pass (blue)*, or Form [USM-569](#) must be escorted at all times.
  - b. USMS employees or contractors who have been issued a BID may escort visitors.
  - c. Escorts must meet their visitors at the Security Contractor Station located at 1750 Crystal Drive. The escort will sign the Record of Visitors.
  - d. Escorts must remain with their visitor at all times without exception. If the visitor requires the use of restroom facilities, the escort will unlock the door and remain outside until the visitor is finished.
  - e. Escorts will accompany their visitor to the building exit and ensure that the identification badge is turned into the Security Contractor.
6. Suspicious Event
- a. All USMS employees must keep Form [USM-531D](#), *Suspicious Activity Report*, in their office or work station.
  - b. Suspicious activity should be reported to the Security Contractor Control Room at (b) (7)(E) [REDACTED]
  - c. Reports will be made using Form [USM-531D](#).
  - d. (b) (7)(E) [REDACTED]
    - 1) (b) (7)(E) [REDACTED]
    - 2) (b) (7)(E) [REDACTED]
    - 3) (b) (7)(E) [REDACTED]

- 4) (b) (7)(E)
- 5) (b) (7)(E)
- 6) (b) (7)(E)

e. Telephonic Threat:

- 1) All USMS employees must keep Form [USM-531B](#), *Bomb Threat Checklist*, near their telephone.
- 2) In the event of a suspicious or threatening call, Form [USM-531B](#) will be used to record as much information as possible.
- 3) All suspicious or threatening calls will be reported to the Security Contractor Control Room at (b) (7)(E)

f. Suspicious Mail:

- 1) All employees and contractors must keep Form [USM-531C](#), *Suspicious Package Checklist*, in their office or workstation.
- 2) Mail and packages are screened at the USMS warehouse in accordance with the Security Contractor post orders.
- 3) Mail is not opened at the USMS warehouse.
- 4) Not all hazards that can be sent in the mail are readily apparent during x-ray screening.
- 5) USMS employees and contractors should exercise caution when opening mail, especially mail from unknown return addresses or penal institutions.
- 6) (b) (7)(E)
- 7) (b) (7)(E)
- 8) (b) (7)(E)
- 9) (b) (7)(E)
  - a) (b) (7)(E)
  - b) Complete Form [USM-531C](#).
  - c) (b) (7)(E)

d) (b) (7)(E)

e) (b) (7)(E)

g. Inappropriate Communications

- 1) Inappropriate communications directed at USMS employees or contractors whether written or verbal will be reported to the Chief Inspector for Headquarters Security.
- 2) After duty hours, inappropriate communications will be reported to the Security Contractor Control Room at (b) (7)(E)
- 3) Inappropriate communications received because of an USMS employee's or contractor's employment will fall under the jurisdiction of the USMS.
- 4) Investigations will be conducted in accordance with USMS Policy Directive 10.3, [\*Protective Investigations\*](#).
- 5) Inappropriate communications received in or on USMS-controlled space may be investigated by the USMS if it is determined that it is in the best interest of the Agency to do so.
- 6) If required, special security arrangements may be implemented at the discretion of the SPM.

h. Emergency procedures for USMS Headquarters are specified in the Occupant Emergency Plan in accordance with [\*Executive Order 12656, Assignment of Emergency Preparedness Responsibilities\*](#) (as amended). All USMS employees and contractors are required to abide by all alarms and emergency plans.

i. The Facility Security Committee (FSC) will serve as an advisory body for the SPM in accordance with the standards set by the Interagency Security Committee and will include the SPM and representatives from:

- 1) Headquarters Security Branch;
- 2) Physical Security Operations, OFCC;
- 3) Building Liaison, OFCC;
- 4) Security Contractor;
- 5) Vornado (or current property manager);
- 6) DON;
- 7) Crystal Square Three;
- 8) Crystal Square Four;
- 9) Crystal Mall;





# United States Marshals Service POLICY DIRECTIVES

## TACTICAL OPERATIONS

### 17.7 PERSONNEL SECURITY

- A. Proponent:** Office of Security Programs (OSP), Tactical Operations Division (TOD).  
Telephone: 202-307-5129, Fax: 703-603-7001.
- B. Purpose:** This policy sets forth responsibilities of the United States Marshals Service (USMS) personnel security and suitability programs.
- C. Authority:** The Director's authority to direct and supervise all activities of the USMS is set forth in [28 U.S.C. § 561\(g\)](#) and [28 C.F.R. § 0.111](#). Additional authority is derived from the following: [28 U.S.C. § 564 and 566](#), [18 U.S.C. § 3053](#), and [FRCP Rule 4\(d\)\(1\)](#); Executive Orders [10450](#), [12968](#), [13467](#), [13488](#), and [13526](#); [5 C.F.R. Parts 731, 732, 736](#), and [2635](#); [28 C.F.R. Part 17](#); [5 U.S.C. § 552a](#), and [15 U.S.C. § 1681](#); [The Intelligence Reform and Terrorism Prevention Act \(IRTPA\) of 2004](#); [Homeland Security Presidential Directive-12 \(HSPD-12\)](#) and [Federal Information Processing Standard Publication 201 \(FIPS 201\)](#); Department of Justice (DOJ) Orders [2600.2D](#), [2610.2B](#), and [2640.2F](#); and [DOJ Security Program Operating Manual \(SPOM\)](#).
- D. Policy:**
1. In accordance with Office of Personnel Management (OPM) regulations contained in [5 C.F.R. § 731](#) and [5 C.F.R. § 732](#), all position descriptions must be evaluated and assigned to a position designation level by the Human Resources Division (HRD) (Refer to [Attachment A](#) for Position Designation levels).
  2. If the position requires access to National Security Information (NSI), Form [USM-561](#), *Request for Security Clearance to Access National Security Information*, is required. This must reflect the justification for the clearance request. The clearance levels are Confidential, Secret, Top Secret, and Sensitive Compartmented Information.
  3. The background investigation process begins upon receipt of a Tentative Offer Letter (TOL) package, which includes a copy of the tentative offer letter, the position designation level, and Form [USM-561](#) if a clearance is required. For applicant cases, the TOL package includes copies of the completed employment reference checks and a completed copy of Form [OF-306](#), *Declaration for Federal Employment Form*.
  4. The final position designation determines the type of investigative form the applicant or employee must complete, as well as the type of background investigation required. The investigative forms include:
    - a. Form [SF-85](#), *Questionnaire for Non-Sensitive Positions*;
    - b. Form [SF-85P](#), *Questionnaire for Public Trust Positions*; or
    - c. Form [SF-85PS](#), *Supplemental Questionnaire for Selected Positions*; and

- d. Form [SF-86](#), *Questionnaire for National Security Positions*.
- 5. All USMS positions are filled only by persons who have undergone a pre-appointment background investigation to determine whether or not the employment of such individuals is clearly consistent with the efficiency of the service and, if required for the position, in the interests of national security.
- 6. Background investigations and eligibility determinations are reciprocally accepted by the USMS unless there is information indicating that an employee may not satisfy the core duties of the new position. The investigation must be conducted based on the appropriate security form and meet the current requirement of the position designation.

**E. Responsibilities:**

**1. Security Program Manager (SPM):**

- a. The SPM or a designee makes Employment Suitability and Security Approvals for public trust positions based on the appropriate investigations and in accordance with [Executive Order 10450](#) and OPM guidance. The SPM or designee reports the final adjudication determination to OPM within 90 days of the date of the completed investigation as required by [Executive Order 10450](#).
- b. The SPM or a designee makes trustworthiness determinations for eligibility for access to classified information based on the appropriate investigation and in accordance with [Executive Order 12968](#). The SPM or designee reports the final adjudication determination to OPM within the mandated timeframe in accordance with the [Intelligence Reform and Terrorism Prevention Act of 2004](#).
- c. The SPM under delegation by DOJ makes the final determination for granting Employment Security Approvals and national security clearances to USMS employees.
- d. The Heads of Department Components or designees are responsible for ensuring that every employee occupying a position within their organization has been the subject of the requisite investigation (unless a specific waiver has been granted in accordance with paragraph [F.3.](#)), and that the employee's service in that position is advisable in the interest of national security and promotes the efficiency of the service.
- e. OSP maintains official records of the security clearance levels and background investigation data for all USMS employees and contractors. Intern files are maintained for one year following their background approval date.
- f. DOJ Security Staff has the authority to grant and certify special access clearances. DOJ also maintains the authority to grant clearances to all political appointees and attorneys within DOJ.

**F. Procedures:**

**1. Employment Eligibility:**

- a. Non-United States Citizens: DOJ gives strong priority to hiring United States citizens and nationals. Any applicant who is not a United States citizen must be from a country allied with the United States and may only be hired if certain requirements are met.

- b. Dual Citizenship: DOJ components may hire a United States citizen who holds dual citizenship with a foreign country; however, how the applicant has obtained or exercised his/her dual citizenship status is considered in the decision to grant or deny eligibility for access to NSI. For citizenship requirements, refer to [DOJ Order 2610.2B](#) and OPM Policy.
- c. Residency Requirement: In order to ensure adequate investigative coverage, [DOJ Order 2610.2B](#), *Personnel Security Order*, requires that applicants have lived in the United States for a total of 3 out of the last 5 years prior to applying for a position, worked for the United States overseas in a federal or military capacity, or been a dependent of a federal or military employee serving overseas.

2. **Pre-Employment Process:**

- a. Employment reference checks are obtained from employment within the last 3 years and any federal employment in the last 7 years. Form [USM-164](#), *Applicant Appraisal Questionnaire Form*, or subsequent employment reference check forms should be used. Reference checks may be conducted by telephone.
- b. Upon receipt of the TOL package, which includes the TOL, position designation level, Form [USM-561](#), and copies of employment reference checks for applicants, OSP initiates the investigative process.
- c. OSP initially determines if there is an investigation that meets the investigative requirement of the position and requests any necessary security forms.
- d. OSP conducts preliminary record checks and resolves any developed issues prior to initiation of a pre-appointment background investigation on applicants.

3. **Waivers:**

- a. Waivers to the required pre-employment background investigation may be considered in unusual or emergency circumstances. As set forth below, waivers may be requested for administrative or contractor positions.
- b. Waivers are not considered for positions designated as Special Sensitive or for applicants for operational positions.

4. **The Procedure for Requesting a Waiver for a Federal Applicant:**

- a. An Associate Director (AD), United States Marshal (USM), or designee must submit a waiver memo that states the unusual or emergency circumstances that warrant a waiver of the required pre-appointment background investigation. The completed reference checks must be included, if not previously sent. The waiver request should be submitted to the attention of: Office of Security Programs, at [OSP-Applicant@usdoj.gov](mailto:OSP-Applicant@usdoj.gov).
- b. OSP must have received the completed security package from the applicant.
- c. The required level of investigation must be scheduled by OPM.
- d. OSP must confirm that initial record checks have been completed with favorable results.

5. **The Procedure for Contractor Waivers:**

- a. The Contracting Officers Representative (COR) or designee submits a written memo stating the unusual or emergency circumstances for the request to the attention of the OSP, at [OSP-Contractor@usdoj.gov](mailto:OSP-Contractor@usdoj.gov).
- b. OSP must have received the completed security package from the applicant.
- c. The required level of investigation must be scheduled by OPM.
- d. OSP initial record checks must have favorable results.

6. **Adjudicative Notification Process:**

- a. For applicants, permanent, temporary, full-time, and part-time USMS employees, OSP notifies HRD of its final suitability and security adjudicative decision, as applicable.
- b. For Applicant Non-selection, OSP submits the recommendation to non-select to Office of General Counsel and HRD for concurrence. If they concur, HRD notifies the applicant and OSP. If they do not concur OSP will continue with the adjudication process.
- c. Decisions on interns (refer to Procedure [Section 8](#)) are sent to the requesting official.
- d. OSP sends final approval or disapproval memos on Contractor applicants (refer to 17.7, Procedures, [Section 9](#), below) to the appropriate COR, or designee in the district/division.

7. **Access to NSI:**

- a. **Requests for Access to NSI:** All requests for access to NSI (security clearances and special access clearances) must be submitted to [OSP-employee@usdoj.gov](mailto:OSP-employee@usdoj.gov) using Form [USM-561](#). Since access to NSI is based on a strict, need-to-know basis, the request must contain a detailed justification of the need for access and the level of access requested.
- b. **Clearance Certifications:** Employees who attend meetings or other events that require a clearance should send a request to [OSP-employee@usdoj.gov](mailto:OSP-employee@usdoj.gov) as soon as possible in order to have their clearance certified to the hosting agency. Notification must include the name of the agency needing the certification, the name and telephone number of the meeting point of contact, and the purpose and date of the meeting or event.
- c. **Clearance Suspensions:** A security clearance may be suspended as a result of adverse information regarding an employee indicating that suspension is necessary based upon the interests of national security. USMs and ADs are required to notify the SPM of any adverse information regarding an employee which may have a bearing on that employee's continued eligibility for access to NSI. A clearance suspension is immediately referred to HRD for appropriate action.
- d. **Administrative Withdrawal:** Clearances are to be administratively withdrawn when there is no longer a need for access to NSI. Notification must be provided to OSP when an employee no longer needs access to NSI.



- e. **Clearance Revocations:** A decision to revoke an existing security clearance may be made following a full review of the adverse information, to include affording the affected employee due process under the provisions of Section 5.2 of [Executive Order 12968](#) and [28 C.F.R. § 17.47](#).
- f. **Clearance Denial:** A decision to deny a request for a security clearance may be made following a full review of the adverse information, to include affording the applicant or employee due process under the provisions of Section 5.2 of [Executive Order 12968](#) and [28 C.F.R. § 17.47](#).
- 8. **Student Volunteer Interns:** The Student Volunteer Intern position is Low Risk, and as such the background investigation for these candidates consists of a records check as deemed appropriate by the USMS. Once approved, this check is good for 1 year from the date a favorable decision was made.
- 9. **Contractors and Guards:** All USMS contract personnel must undergo a background investigation comparable to that of a USMS employee occupying a position of the same sensitivity level or having access to the same or similar types of information. Contractors are processed in a manner similar to USMS employees. However, contractors who require access to classified NSI are cleared in accordance with the requirements of the National Industrial Security Program, in which the USMS is a participant.
- 10. **Other Personnel:** All non-USMS personnel who work at the USMS, or have access to USMS space, must have a federal background investigation favorably adjudicated and accepted under reciprocity by OSP.
- 11. **Reinvestigations:** Pursuant to [DOJ Order 2610.2B](#), the incumbent of every position within the USMS is required 5 years after his/her initial background investigation, and at least once in every subsequent 5-year period, to undergo a background reinvestigation.
- 12. **Types of Background Investigations:**
  - a. **National Agency Check (NAC):** A required component in all investigations consisting of searches of the OPM Suitability/Security Investigations Index, Federal Bureau of Investigation (FBI) Criminal History Records, FBI Headquarters investigation files, Defense Clearance and Investigations Index (DCII), and other sources as necessary to cover specific areas of a subjects background.
  - b. **National Agency Check with Law and Credit (NACLC):** A NACLC consists of a NAC, law enforcement checks for the past 5 years (inquiry or records), and a credit search for the past 7 years.
  - c. **National Agency Check and Inquiries (NACI):** A NACI consists of a NAC, written inquiries and record searches covering specific areas of an individual's background during the past 5 years.
  - d. **Minimum Background Investigation (MBI):** A MBI consists of a NAC, personal subject interview, written inquiries (5-year coverage for employment, education and law enforcement, and 3-year coverage for residence), and a credit search covering 7 years.
  - e. **Background Investigation (BI):** This type of investigation consists of a NAC, personal subject interview, credit search, written inquiries of selected sources and record sources, and personal interviews covering specific areas for 5 years.
  - f. **Periodic Reinvestigation (PRI):** This investigation covers specific areas up to

the past 5 years and includes a personal interview.

- g. **Single-Scope Background Investigation (SSBI):** An SSBI consists of a NAC, personal interviews of subject and sources, credit search, written inquiries, birth or citizenship verification, and record searches covering specific areas of subject's background during the past 7 to 10 years.
- h. **Single-Scope Background Investigation-Periodic Reinvestigation (SSBI-PR):** The required 5-year update investigation for the SSBI consisting of a search from the United States Treasury Department's financial data base, a NAC, personal subject interview, former spouse interview, written inquiries of selected sources, record sources and personal interviews covering specific areas for the past 5 years and a credit search covering 7 years.
- i. **PHASED-PR:** An alternate investigation that may be requested as a 5-year update for the SSBI which consists of a search from the United States Treasury Department's financial data base, a NAC, personal subject interview, written inquiries of selected sources, record sources and personal interviews covering specific areas for the past 5 years, and a credit search covering 7 years.
- j. **Access National Agency Check and Inquiries (ANACI):** An investigation which includes a National Agency Check (NAC), 5-year written inquiry coverage for employment, education, residence, references, and law enforcement (inquiry or records), and a credit check covering 7 years.

**G. Definitions:**

- 1. **Employment Security Approval:** A favorable adjudication by the SPM or designee of a background investigation on an employee/applicant and a determination based on the available information that the individual is honest, trustworthy, loyal, and free from coercion. This security approval is made after the favorable suitability determination.
- 2. **National Security Positions:** Those positions that involve activities of the Government that are concerned with the protection of the nation from international terrorism, foreign aggression, or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with the preservation of the military strength of the United States, as well as those positions that require regular use of, or access to, classified information.
- 3. **Need-to-Know:** A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized government function.
- 4. **Nondisclosure Agreement (SF-312):** A contractual agreement between the United States Government and an employee with access to classified information, in which the cleared employee agrees never to disclose classified information to an unauthorized person. Form [SF-312](#), *Classified Information Nondisclosure Agreement*.
- 5. **NSI Access Eligibility:** An administrative decision based on a determination by the SPM or designee to grant an individual access to classified information when a specific need-to-know exists.
- 6. **Public Trust Position:** A position where action or inaction by the person occupying the position could affect the integrity, efficiency, and effectiveness of the service.

7. **Reinvestigation:** An updated investigation based on position risk and or position sensitivity level to determine continued employment and/or NSI access eligibility.
8. **Suitability Determination:** A determination, based on character or conduct, of whether a person is likely to be able to carry out the duties of a federal position with appropriate integrity, efficiency, and effectiveness.

H. **References:** None.

I. **Cancellation Clause:** This policy directive supersedes *Attachment A*, Policy Directive 17.6, *Security Programs Manager*.

J. **Authorization and Date of Approval:**

**By Order of:**

**Effective Date:**

/S/  
Stacia A. Hylton  
Director  
U.S. Marshals Service

05/28/2013

## Policy Directive 17.7, *Personnel Security*, Attachment A.

### Position Designation Levels:

The Office of Personnel Management regulations contained in [5 C.F.R. Parts 731](#) and [732](#) require that all positions descriptions be evaluated and be assigned a position sensitivity level. Each position will be designated as Special Sensitive, Critical Sensitive, High Risk, Moderate Risk, or Low Risk according to that position's impact upon the efficiency of the United States Marshals Service (USMS) and national security. Similarly, all USMS contract positions will be designated at one of the above levels following an evaluation of the contract statement of work. The categories of position sensitivity are:

1. **Special Sensitive:** Positions within the USMS will be those national security positions that:
  - a. Involve the highest degree of trust to include senior Headquarters and district management officials.
  - b. May require access to, or afford ready opportunity to gain access to any classified information that is controlled by special access procedures (e.g., access to Sensitive Compartmented Information granted by the U.S. intelligence community).
  - c. Involve duties in the Witness Security Program.
  - d. Require access to any other category of information having the potential for significant impact upon national security, as designated by the Director.
  - e. Employees who are selected for Special Sensitive positions must undergo a Single Scope Background Investigation (SSBI) which must be favorably adjudicated prior to assuming the position. Employees are required to submit security forms every 5 years so that an SSBI Periodic Reinvestigation (SSBI-PR) may be initiated. Interim clearances are approved for USMS employees accepting a special sensitive position through the merit promotion process.
2. **Critical Sensitive:** Positions within the USMS will be those national security positions that require access or afford ready opportunity to gain access to Top Secret National Security Information (NSI) and material as described in [Executive Order 12968](#) or as amended. Employees in Critical Sensitive positions must undergo a SSBI prior to their initial appointment and a SSBI-PR reinvestigation every succeeding 5 years.
3. **High Risk:** Public trust positions are those sensitive positions that have the potential for exceptionally serious impact involving duties especially critical to the USMS or a program mission with broad scope of policy or program authority, but do not require access to classified NSI. These positions typically involve law enforcement duties; policy development or implementation; higher level management assignments; independent spokespersons or non-management positions with authority for independent action; significant fiduciary and procurement authority and responsibilities; ADP-computer positions responsible for the planning, direction, and implementation of a computer security program; the direction, planning, and design of a computer system, including the hardware and software; or, accessing a system during the operation or maintenance in such a way, with relatively High Risk to cause grave damage or realizing significant personal gain. (Refer to [OMB Circular A-130](#), *Management of Federal Information Resources*, for computer positions that are High Risk)
  - a. Employees in High Risk positions undergo a BI prior to their initial appointment, and an ANACI reinvestigation every succeeding 5 years.

4. **Moderate Risk:** Public trust positions are those sensitive positions that have the potential for moderate to serious impact involving duties very important to the USMS or program mission with significant program responsibilities and delivery of customer services to the public. Including, assistance to policy development and implementation, mid-level management assignments, non-management positions with authority for independent or semi-independent action; delivery of service positions that demand public confidence or trust, ADP-computer positions of a lesser degree of risk than that required for High Risk positions, Freedom of Information/Privacy Act duties, and positions that require access to Grand Jury information.
  - a. Employees in Moderate Risk positions must undergo a Minimum Background Investigation (MBI) prior to their initial appointment, and a National Agency Check with Law and Credit (NACLC) reinvestigation every succeeding 5 years.
5. **Low Risk:** Public trust positions are those non-sensitive positions that do not fall into any of the above categories and involve limited potential for impact upon the USMS mission. Low Risk positions require a National Agency Check and Inquiries.
6. **Low Risk-Intermittent:** Positions that are intermittent, seasonal, per diem, or temporary, are not to exceed an aggregate of 180 days in either a single continuous appointment or series of appointments do not require a background investigation. The USMS will conduct checks as it deems appropriate to ensure the suitability of the person.



## United States Marshals Service **POLICY DIRECTIVES**

### **TACTICAL OPERATIONS**

#### **17.8 BADGES AND CREDENTIALS**

- A. Proponent:** Tactical Operations Division (TOD), Telephone: 202-307-9485; Fax: 202-307-9366.
- B. Purpose:** This policy directive outlines the administrative procedures for the Badge and Credential Program (BCP) and procedures for the safeguarding of badges and credentials against misuse.
- C. Authority:** The Director, United States Marshal Service (USMS) is authorized pursuant to [18 U.S.C. § 701](#) and Department of Justice (DOJ) Order [2610.1A](#) to create credentials for employees of the USMS.
- D. Policy:**
- 1. Use of Badges and Credentials:**
    - a. While on duty, all USMS operational employees must carry their credentials identifying themselves as duly authorized federal law enforcement officials.
    - b. USMS badges and credentials may only be used by the person to whom they are issued and for actions performed in the line of official duty. Credentials are issued only to permanent USMS employees. Exceptions to this policy may only be made by the Director.
    - c. Employees may not alter or change the officially-issued credential case in any way including, but not limited to, affixing any unauthorized item or writing to it.
    - d. Employees are responsible for safeguarding their USMS badges and credentials. Employees may be required to pay for actual replacement or may be disciplined in the case of loss, theft, or unauthorized destruction of badges and credentials. Employees must store their badges and/or credentials in a secure location affording reasonable safeguards against theft or loss.
  - 2. Issuance and Surrender:**
    - a. Credentials signed by a previous USMS Director remain valid.
    - b. Operational employees are issued one set of credentials, one credential badge, and one belt badge with the same number as their credentials.
    - c. Employees serving an interim or temporary appointment as a United States Marshal (USM) or the Director receive USM credentials with a gold case and belt badge. If a current Deputy United States Marshal (DUSM) is serving as an interim USM, he/she may retain his/her current USMS-issued silver badge/credential during the appointment, utilizing USMS property controls.

- d. USMS law enforcement service badges are not issued as mementos. Memento USMS badges can be requested, in writing, from the BCP. Refer to Section E.8, memento badges.
  - e. Upon exiting federal service, employees must surrender all badges and credential cards in their custody to the USM or appropriate supervisor.
3. **Reproduction and Replication:** The Office of Security Programs (OSP), TOD, is the only entity authorized to purchase USMS law enforcement service badges. No individual or entity may reproduce and/or replicate official USMS insignia/indicia without written approval from the Director (refer to Policy Directive 1.3, [USMS Name and Insignia](#)).
- a. USMS employees, guards, contract personnel, and other individuals are not authorized to carry or display unofficial replicas of USMS badges while performing duties on behalf of the USMS.
  - b. Employees having knowledge of unauthorized badge or credential reproduction, commercial or otherwise, must report it immediately to the BCP, Office of Inspection (OI), and the Office of General Counsel (OGC).
  - c. USMS personnel are prohibited from creating new USMS duty badges or ordering USMS duty badges or credential cases directly from manufacturers. All requests for replacement badges, the creation of new duty badges, and the ordering of credential cases are coordinated by BCP.

**E. Procedures:**

1. **New-issue Badges and Credentials for Permanent Employees:**
- a. The USM, Chief Deputy United States Marshal (CDUSM), or Assistant Director (AD) requests USMS badges and credentials for new employees, employees who have never had badges or credentials, or for Special Deputies whose credentials have expired.
  - b. The USM, CDUSM, or AD signs and submits Form [USM-287](#), *Request for Badge/Credential Action*, along with two color pictures of the employee and a credential signature sheet signed by the employee in black ink. Employees must sign the signature sheet exactly as the name will appear on the credential.
  - c. BCP forwards the completed credentials, credential badge, and the belt badge to the requesting USM, CDUSM, or AD. The completed credentials and/or badges are accompanied by Form [USM-288](#), *Badge/Credential Hand Receipt*. The individual to whom the credentials and/or badge are issued must sign Form [USM-288](#) and immediately return the signed form to BCP.
  - d. TOD administers the Special Deputy Program (SDP) and may authorize USMS badges and credentials for Special Deputies who are cleared, full-time Task Force Officers (TFOs) working on a district or regional task force for a period of 1 or more years. The request for Special Deputy badge and credentials should include: Form [USM-287](#) with at least one numerical identifier (i.e., social security number); copy of Special Deputy Authorization; copy of Form [USM-3A](#), *Application for Special Deputation*; copy of approved PSB suitability memo; two passport-size photos, and signature page. All documents are sent to Badge and

2. **New-Issue Badges and Credentials for Political Appointees:**

- a. The official appointment memorandum from the Attorney General serves as the request for the issuance of the badge and credentials to the appointee.
- b. BCP must receive the appointment memorandum, along with two passport-size photographs and a credential signature sheet signed by the appointee in black ink. The appointee must sign the signature sheet exactly as the name will appear on the credential.
- c. BCP retains the competed badge and credential until the appointee has been confirmed. At such time, the appointee is presented with the badge and credential. BCP requires Form [USM-288](#). The appointee must sign the form and return to BCP.

3. **Replacement and Updated USMS Badges and Credentials:**

- a. Replacement badges and credentials may be requested by a USM, CDUSM, or AD using the same procedures outlined for new-issue badges and credentials. The USM, CDUSM, or AD requests the replacements after the DUSM reports for duty at the new office. All requests must be sent to the BCP.
- b. The USM, CDUSM, or AD requests replacement or updated credentials using Form [USM-287](#) when one or more of the circumstances described below occurs.
  - 1) Change of position title which necessitates a change to only the authority (top) card of the credential;
  - 2) Loss of badge(s) and/or credential;
  - 3) Change of name of the individual to whom the credential is issued. Explain reason(s) in attachment to the Form [USM-287](#). Send a new signature sheet and new photographs; and
  - 4) Change in appearance of the individual to whom the credential is issued to the extent that the photograph on the existing (bottom) credential sheet bears little resemblance to the individual. Include a new signature sheet and new photographs.

4. **Lost or Stolen Badges and Credentials:**

- a. **Reporting Lost or Stolen Badges and Credentials:** The individual to whom a USMS badge(s) or credential is issued is responsible for immediately reporting the loss or theft of the badge(s) or credential to the USM and to BCP, TOD located at USMS Headquarters. The USM, CDUSM, or AD immediately notifies the local police and the local office of the Federal Bureau of Investigation (FBI). Loss includes misplacement or any other circumstance that results in the employee no longer having physical possession of the badge(s) or credential.
- b. **Replacing Lost or Stolen Badges and Credentials:** The USM, CDUSM, or AD requests replacement of lost USMS badges and credentials on Form [USM-287](#)



following the procedures outlined for new badges and credentials (see above). Because badges and credentials are numbered in sets (credential and two badges), the loss of the badge or credential requires the issuance of another set bearing a different number.

**5. Accountability:**

- a. USMS badges and credentials are issued directly to individual employees by the BCP. BCP maintains records that document current badge issuance and provide the official inventory record of receipt for badge issue.
- b. At the beginning of the calendar year, every district and Headquarters division will conduct an inventory of badges and credentials (including Special Deputy badges) issued to district and division personnel and certify the results to the Assistant Chief, BCP by e-mail, by March 1 of each year.

**6. Return of Badges and Credentials:**

- a. Upon an employee terminating employment of his/her federal service by retirement, the employee returns all badges and credentials to the appropriate USM, CDUSM, and/or AD. Upon return of the issued badges and credentials to the USM, CDUSM, and/or AD notifies BCP. The USM, CDUSM, and/or AD returns the employee's badges and credentials to the BCP as soon as possible (see below).
- b. When an employee terminates federal service for any reason other than retirement (i.e., resignation, transfer outside the USMS, death, expiration of appointment, etc.), the USM, CDUSM, or AD returns the employee's credential and badge to the BCP as soon as possible.
- c. All badges and credentials must be returned in person to the official duty station or via registered mail or any commercial parcel delivery service that provides receipts and has the capability to track missing or lost packages.
- d. When a political appointee's term ends, the Office of the Director notifies the BCP. The appointee must return the gold badge and credential to the BCP as soon as possible and indicate whether he/she is returning to a USMS position, departing from the Agency or retiring.
  - 1) Appointee returning to a USMS position or departing from the USMS is presented with the gold duty badge to be carried as of the date of separation encased in Lucite (at the expense of the district). The belt badge must be returned, unless encased in Lucite. If the appointee desires the belt badge to be encased in Lucite, he/she incurs the cost.
  - 2) Appointee retiring from the USMS on an immediate federal annuity directly from the position of Director or USM is issued the gold duty badge to be carried as of the date of separation and retirement credentials. An "R" will be engraved behind the badge number on the duty badge. The belt badge is encased in Lucite. The cost is incurred by the district or Headquarters division.

7. **Retirement Badges and Credentials:** Retirement duty badges and credentials retained by retired employees as mementos are addressed in Policy Directive 17.9, [Retirement Badge and Credential](#).
8. **USMS Memento Badges:** Official duty badges are not to be given as mementos. The BCP issues a specially designed badge for this purpose. Only the following persons are eligible to receive memento badges:
  - a. Federal, state, and local dignitaries and officials that have made a substantial contribution to the nation or USMS; or
  - b. USMS employees who are departing from the Agency or retiring. Contractors are not eligible recipients.
9. Workplan/appropriated funds may be used to purchase memento badges.
10. Contact the BCP for ordering information.

**F. Responsibilities:**

1. **USM, CDUSM, and AD:** Responsible for requesting, retrieving, and returning USMS badges, credentials, and other issued identification from district employees or contractors who are hired, terminated, or who no longer have a need for such identification.
2. **Employees:** Responsible for safeguarding USMS badges and/or credential and returning badges and credentials to the USMS upon termination of employment.
3. **AD, TOD:** Responsible for authorizing changes to the list of approved credential titles and the issuance of badges and credentials.

**G. Definitions:**

1. **Credentials:** Tangible means of identifying all permanent, full-time or part-time employees that are issued for the duration of employment and are considered accountable property. Credentials include the top and bottom cards.
2. **Badges:** Metal emblems that formalize the identification of operational employees who are issued law enforcement credentials. The USMS credentials badge and the belt badge contain the same numbers as the corresponding credential. A badge may not stand alone, but must be confirmed by a matching law enforcement credential.
3. **Memento Badge:** A non-service USMS badge, specially designed for the purpose of a souvenir.

**F. Cancellation Clause:** This policy directive supersedes Policy Directive 3.7, *Personnel Security, Badges and Credentials*.

**G. Authorization and Date of Approval:**

**By Order of:**

**Effective Date:**

          /S/            
Stacia A. Hylton  
Director  
U.S. Marshals Service

          10/14/11



## United States Marshals Service POLICY DIRECTIVES

### TACTICAL OPERATIONS

#### 17.9 RETIREMENT BADGE AND CREDENTIAL

- A. Proponent:** Badge and Credential Program (BCP), Tactical Operations Division (TOD).  
Telephone: 202-307-9485, Fax: 202-307-9366.
- B. Purpose:** This policy directive describes the use of and eligibility for United States Marshals Service (USMS) retirement badges and retirement credentials.
- C. Authority:** The USMS Director is authorized pursuant to [28 U.S.C. § 561](#) to create credentials for retired employees of the USMS. [18 U.S.C. § 926C](#) addresses identification for retired law enforcement personnel.
- D. Policy:** All employees of the USMS who are eligible to retire under the [Civil Service Retirement System](#) (CSRS) or the [Federal Employees Retirement System](#) (FERS) may be issued retirement credentials. Operational employees may also be issued a retirement badge.
1. **Retirement Credentials Do Not:**
    - a. Convey any law enforcement powers and/or authorities; any representation of such by the holder constitutes impersonation of a federal officer;
    - b. Permit the holder to carry a concealed firearm; or
    - c. Entitle the holder to any rights or privileges not enjoyed by the general citizenry.
  2. **Eligibility for Retirement Credentials:**
    - a. **United States Marshals (USMs):** Retiring USMs who have been appointed by the President or, in the case of the District of the Virgin Islands, by the United States Attorney General, to a term in office as a United States Marshal (USM), may be issued retirement credentials, provided that they are retiring from the USMS directly from the position of USM and that, before their separation, for an aggregate of 10 years, they were authorized by law to engage in or supervise the prevention, detection, investigation, prosecution, or incarceration of any person for any violation of law and had statutory powers of arrest.
    - b. **Law Enforcement Employees:** Retiring law enforcement employees, other than USMs, may be issued retirement credentials upon retiring from the USMS under the [CSRS](#) or [FERS](#) retirement system.
    - c. **Service Connected Disability:** Law enforcement employees who have completed their probationary period and have separated from the USMS due to a service-connected disability, as determined by the USMS, may be issued retirement credentials.

- d. **Administrative Employees:**
  - 1) Administrative employees may be issued administrative retirement credentials upon retiring from the USMS under [CSRS](#) or [FERS](#) retirement system.
  - 2) Retiring administrative employees will be eligible to receive the Lucite encased credentials carried by the employee as of the date of retirement. The cost will be borne by the USMS.
- 3. **Eligibility for Retirement Badge:**
  - a. **USM Political Appointees:** Retiring USMs or Directors who have been appointed by the President or, in the case of the District of the Virgin Islands, by the United States Attorney General to a term in office as a USM or Director may be issued the gold duty badge carried as of the date of separation. An "R" or the word RETIRED will be engraved on the reverse of the duty badge. The badge may be encased in Lucite or provided loose. The cost of this will be borne by the USMS.
  - b. **Law Enforcement Employees:** Law enforcement employees, other than USMs, who retire under [CSRS](#) or [FERS](#) may be issued the silver badge carried as of the date of separation. An "R" or the word RETIRED will be engraved on the back of the badge. The badge may be encased in Lucite. The cost of this will be borne by the USMS.
- 4. **Separated Employee Identification Cards:** May be given to USMS law enforcement personnel who:
  - a. Separate from the USMS in good standing;
  - b. Do not leave the USMS to go to another law enforcement agency; and
  - c. Before their separation and for an aggregate of 10 years, were authorized by law to engage in or supervise the prevention, detection, investigation, prosecution, or incarceration of any person for any violation of law and had statutory powers of arrest.
- 5. **Use of Retirement Badge and Credential:**
  - a. The retirement badge and credential or the badge encased in Lucite does not convey any law enforcement powers and/or authorities; any representation of such by the holder constitutes impersonation of a federal officer. Possession of retirement credentials does not entitle the holder to any rights or privileges not enjoyed by the general citizenry except as allowed by the [Law Enforcement Officers' Safety Act](#).
  - b. Retiring operational employees will be required to sign a Memorandum of Understanding (MOU) and Form [USM-288](#), *Hand Receipt*, which is retained by the BCP coordinator.
- 6. **Control of USMS Issued Materials:** District management will account for and forward by controlled mail to BCP all USMS-issued and -controlled badges and credentials at the time of employee separation. Requests for retirement badge and/or credentials should be sent to BCP 6 weeks in advance of the date they are required for presentation to the retiring employee.

7. **Lost or Stolen Retirement Badges and Credentials:**

- a. Retirement badges and credentials remain the property of the USMS at all times
- b. The holder must report the loss of a retirement badge and/or retirement credential in writing to the nearest district office.
- c. After lost or stolen retirement badges and/or credentials are reported to TOD, they will be posted as such on [National Crime Information Center](#).

E. **Responsibilities:**

1. **USMs, Chief Deputy United States Marshals (CDUSMs), and Assistant Directors (ADs):** USMs, CDUSMs, and ADs are responsible for retrieving USMS badges, credentials, and other issued identification from USMS employees upon their retirement; requesting BCP/TOD to prepare retirement badges and credentials at least 6 weeks prior to the employee's anticipated retirement; presenting the retired employee with a retirement badge and/or credential; and returning the employee's duty badge and credentials to USMS Headquarters BCP.
2. **Employees:** The retiring employee is responsible for submitting a new signature card provided by BCP, and two current photographs (plain background) 6 weeks prior to the anticipated retirement date. Dimensions of the photographs must be at least 2 by 2 inches and must include the individual's head and shoulders with the individual facing directly into the camera. Face size must be approximately 3/4 inch horizontally by 1 inch vertically. The individual must be photographed wearing conservative coat, shirt, and tie (for males), and a conservative blouse (for females). Employees are responsible for returning their badges and credentials to the USM, CDUSM, and/or AD on the last day of employment and for executing any required agreements or forms.
3. **AD, TOD:** Responsible for the issuance of retirement badges and credentials and for maintaining appropriate inventory and documentation of these controlled materials.

F. **Definitions:**

1. **Retirement Badge:** Service badge with "R" or the word RETIRED engraved behind number.
2. **Retirement Credentials for Administrative Employees:** Specially designed credentials for retired administrative employees.
3. **Badge:** The last official badge carried by a USMS law enforcement employee.

G. **Cancellation Clause:** This policy directive supersedes Policy Directive 3.7, *Personnel Security, Badges and Credentials*.

H. **Authorization and Date of Approval:**

**By Order of:**

**Effective Date:**

/S/  
Stacia A. Hylton  
Director  
U.S. Marshals Service

6/28/12



# United States Marshals Service POLICY DIRECTIVES

## TACTICAL OPERATIONS

### 17.10 VAULTS, SAFES, AND SECURE STORAGE AREAS

- A. Proponent:** Office of Security Programs (OSP), Tactical Operations Division (TOD).  
Telephone: 202-307-5129, Fax: 202-307-3446.
- B. Purpose:**
1. The United States Marshals Service (USMS) provides secure storage facilities for assorted categories of holdings including, but not limited to, United States Treasury checks, seized property, evidence, witness security records, USMS-owned weapons, ammunition, financial instruments, and other miscellaneous property required for the conduct of official business.
  2. Certain categories of material demand specific access limitations by employees. These categories include, but are not limited to, medical records, test results, certain personnel actions, National Security Information (NSI), investigations, and others. Access stipulation for specific programs will be addressed within the appropriate section of the [Security Program Operating Manual](#) or by other cited guidelines.
- C. Authority:** The Director's authority to establish protocols for USMS vaults, safes, and secure storage areas is derived from [28 C.F.R. § 0.111](#), [Department of Justice \(DOJ\) Order 2620.7](#), [Control and Protection of Limited Official Use Information](#); [DOJ Order 2620.5A](#), [Safeguarding Tax Returns and Tax Return Information](#); [DOJ Order 2600.4](#), [Safeguarding Grand Jury Information](#); and [DOJ Order 2640.1](#), [Privacy Act Security Regulations For Systems Of Records](#).
- D. Policy:** All security equipment (vaults, safes, or secure storage areas) is provided for protection of government property or property under control of the USMS for official purposes. Only materials secured for official purposes may be maintained in these containers. Employees may not store personal items in USMS security equipment. The United States Marshal may not authorize any other person to do so.
- E. Responsibilities:** OSP maintains a record of all combinations to containers protecting classified information within Headquarters.
- F. Procedures:**
1. **Segregation of Materials:** Materials that require protection are usually regulated by laws or other authority. Although every category of material requiring protection and segregation cannot be identified by this policy directive, the principal categories that concern the USMS are:
    - a. NSI (classified information, documents, diskettes containing the information, material, etc.). Classified documents are protected in designated containers as identified in this policy directive. No other materials may be kept in the same container with classified documents;
    - b. Evidence, segregated by case, is protected to ensure that a legal chain of custody is maintained;

- c. Weapons and related items, dangerous materials, and ammunition;
  - d. Seized property of exceptional value;
  - e. Cash and coins (United States and foreign), legal tender, excluding collections, antique, and relic examples;
  - f. Financial instruments, including blank checks, vouchers, travel documents, and other items;
  - g. Restricted materials relating to health, test results, and other matters; and
  - h. Specified law enforcement equipment and equipment of exceptional value, designated for limited use, or susceptible to damage if retained in ordinary storage.
2. **Access Control:** Access control is a documented procedure established by the senior management official that designates which employee (or designated position) may have access to protected materials. Access to certain types of materials, including NSI, requires formal clearance and notification prior to access being granted. Access may be limited to specified areas/containers and may include other restrictions. Access control procedures may involve:
- a. Limiting access to specified employees;
  - b. A key control plan; and
  - c. Changing combinations, as required.
3. **Combinations:**
- a. Combinations to security containers are changed when:
    - 1) Equipment is initially placed in service;
    - 2) A person knowing the combination is transferred to a position that no longer requires access to the information or material kept in the security container;
    - 3) A combination has been subjected to possible compromise; and
    - 4) Lock repair work has been performed by uncleared personnel.
  - b. Combination numbers are committed to memory and recorded on a General Services Administration (GSA) Form [SF-700](#), *Security Container Information*, and then secured.
  - c. Each container is required to have a unique, individual combination. Duplicate combinations may not be used.
  - d. Security containers with combination locks are not to be left with the lock in an unscrambled position or with the combination pre-dialed.
  - e. District offices are authorized to utilize competent, commercial locksmiths only for changing combinations to containers not storing [classified information](#) or



sensitive USMS information. Refer to Policy Directive 17.6.3, Document Security, for the description and definition of protected information.

- f. When security equipment with a built-in combination lock is taken out of service, the lock should be reset to the standard factory combination (b) (7)(E). Security containers taken out of service must be inspected to ensure that no classified or sensitive information remains in the container.
  - g. GSA Form SF-700 should be completed each time a combination is set.
  - h. District offices maintain and secure container combinations in a central location within the district. Classified combinations must be secured in a GSA-approved container.
  - i. The record of combination, GSA Form SF-700, must be protected and accounted for as a classified document in accordance with the Security Program Operating Manual, 6-207.b when the combination protects classified information.
4. **Personal Property:** It is USMS policy that non-work related personal property is not to be stored in USMS vaults, safes, or secure storage areas, except for personally-owned weapons approved for duty under the following conditions:
- a. The employee has requested authorization to carry a personally-owned weapon as their duty weapon;
  - b. All appropriate approvals, qualification standards, and other requirements have been met prior to authorizing the storage of personally-owned weapons in USMS security equipment. Personally-owned weapons cannot be stored in the same safe or security container as classified documents; and
  - c. Personal weapons or other property brought into the USMS office space are brought in at the owner's risk, and the USMS is not liable if lost, damaged, and/or stolen.
5. **Suboffice and Field Office Security Equipment:** The size and scope of responsibilities assigned to these offices is dissimilar throughout the USMS. With the exception of the use of GSA-approved security containers for the storage of classified information and material, security equipment standards are not specified for these offices. The protection standards required at these facilities are not diminished because of location.
6. **Commercial Security Facilities:** Use of commercial security facilities are considered on a case-by-case basis.

**G. Definitions:**

- 1. **Vault:** An enclosed area designed for protection of the articles placed within to prevent unauthorized access. A vault is a permanent (built-in) chamber, equipped with high security walls, floor, and ceiling, and a door fitted with a combination/key/time/or computer-controlled locking system. A security door may be equipped with several locking mechanisms that are used together to effect a superior degree of protection. Refer to the *Requirements and Specifications for Special Purpose and Support Space Manual*, Publication #64, Volumes I, and II, published and updated by the Office of Facilities and Courthouse Construction (OFCC), Management Support Division. Publication #64 defines mandatory construction requirements and specifications.

2. **Safe:** Safes are free standing and permanently installed, or free standing and attached (anchored) in a fixed position, such as:
  - a. **GSA-Approved Security Container:** A container specifically designated for the protection and storage of classified information and materials, as defined in 32 CFR Parts 2001 and 2004, [Executive Order 12958](#) implementing [Classified National Security Information Directive No. 1](#), dated September 22, 2003. GSA-approved security containers may not be used for the storage of any items of intrinsic value while being used for storage of classified material. GSA-approved containers are designated by class, which serves to delineate the protective requirements that they meet. Class 6 containers provide 30 minutes of protection against covert entry and 20 hours of protection against surreptitious entry, but afford no protection against forced entry. Class 5 containers provide the same degree of protection against covert and surreptitious entry, but also provides 10 minutes of protection against forced entry.
  - b. **Weapons Container:** A container designed for the security of weapons, including side arms, shoulder weapons, and related items. Generally, weapons, ammunition, and other ordnance are not protected within the same container. GSA-approved Class 5 weapons containers are generally ideal for storage of weapons and ammunition. However, because security standards do change, the specifications for weapons containers are provided by separate correspondence on request.
3. **Secure Storage Area:** A storage area of segregated space protected by wire mesh partitions, key locks, or other means used to provide a limited degree of protection to articles. A secure storage area may be constructed within a vault for the purpose of segregating various categories of materials, including evidence, seized property, and financial instruments.
4. **Locking File Cabinets:** Containers used for storage of paper files and other material that do not require a high degree of protection. File cabinets are not considered security equipment. File cabinets may be equipped with combination locks, provide fire protection of some degree, and limit access. Locking file cabinets may be used within vaults or secure storage areas to provide segregation of articles. However, the protection is afforded by the vault and not the cabinet locking system.
5. **Redundant Systems:** To achieve a higher degree of protection than can be accomplished with an individual security system or to accomplish segregation of articles, the practice of enclosing one type of security equipment within another (e.g., placing a safe within a vault) is acceptable.
6. **Compartmented Containers:** Various designs of security equipment are available to the USMS. Approved security containers may have individual subcomponents (lock drawers, boxes, etc.). Generally, the subcomponents have individual locking devices. Security containers with these characteristics are considered appropriate for segregating various categories of materials within a single container. Refer to the *Requirements and Specifications for Special Purpose and Support Space Manual*, Publication #64, Volumes [I](#), and [II](#), updated and published by OFCC. Publication #64 defines mandatory construction requirements and specifications.

## H. References:

1. *Requirements and Specifications for Special Purpose and Support Space Manual*, Publication #64, Volumes [I](#), and [II](#), updated and published by OFCC.

2. [Security Program Operating Manual](#) published by the Justice Management Division, DOJ.

I. **Cancellation Clause:** Supersedes Policy Directive 7.4.3, *Vaults, Safes, and Secure Storage Areas*.

J. **Authorization and Date of Approval:**

**By Order of:**

**Effective Date:**

/S/  
Stacia A. Hylton  
Director  
U.S. Marshals Service

10/08/2012



## United States Marshals Service POLICY DIRECTIVES

### TACTICAL OPERATIONS

#### 17.11 SPECIAL DEPUTATION PROGRAM

- A. Proponent:** Special Deputation Unit (SDU), Tactical Operations Division (TOD), Telephone: 202-307-5224, Fax: 202-307-5089.
- B. Purpose:** To establish United States Marshals Service (USMS) policy and procedures concerning the Special Deputation Program.
- C. Authority:** The authority of the USMS to supervise and administer the Special Deputation Program is contained in [28 U.S.C. §§ 566\(c\), 561\(a\), 561\(f\), 509, 510; 28 C.F.R. §§0.111, 0.112, and 0.113](#).
- D. Policy:**
1. Special deputations by the USMS are authorized based upon the needs of the USMS or other agencies that can demonstrate a requirement to enforce federal law or carry a concealed weapon.
  2. Special deputations are not limited to the district of origin and are valid wherever the United States has law enforcement powers. A special deputation may, however, carry restrictions that limit authority to certain duty hours, a specific investigation, a designated location, personal protection, etc. Limits may also include conditions or restrictions for carrying concealed weapons.
  3. The USMS can deputize state and local police officers for [Title 18](#) criminal offenses only. Special deputies are not authorized to participate in federal drug investigations ([Title 21](#)) unless they are also deputized by the Drug Enforcement Administration (DEA) or the Federal Bureau of Investigation (FBI).
  4. Individuals with special deputation have [Title 18](#) authority, as stipulated on Form [USM-3B, Special Deputation Oath of Office, Authorization and Appointment](#), to perform any of the following federal law enforcement functions:
    - a. Seek and execute arrest warrants and search warrants.
    - b. Make arrests without a warrant if there are reasonable grounds to believe that the suspect has violated or is violating federal law.
    - c. Serve subpoenas and other legal writs.
    - d. Monitor Title III Intercepts (electronic surveillance).
    - e. Carry firearms for personal protection or the protection of those covered under the federal assault statutes.

5. **Applicants for Special Deputation must meet the following requirements:**

- a. Be a United States citizen.
- b. Be employed full-time by a federal, state, local, or tribal law enforcement agency, or an agency approved by the Department of Justice (DOJ).
- c. Have successfully completed a basic law enforcement training program. (If deputation is requested to participate in a protection detail, proof of protective detail training is also required.)
- d. Have at least 1 year of law enforcement experience with an agency that has general arrest authority.
- e. Have no domestic violence convictions as defined in [18 U.S.C. § 922\(g\)\(9\)](#) (the Lautenberg Amendment).
- f. Have successfully qualified with an authorized firearm on the USMS or employing agency's approved course of fire within 6 months of application date.
- g. Complete Form [USM-3A](#), *Application for Special Deputation/Sponsoring Federal Agency Information for Special Deputation*. Incomplete applications will not be processed.
- h. Have certified that they have reviewed and agreed to comply with the deadly force policy of the employing agency or the DOJ.
- i. Federal Government employees must be classified in a Law Enforcement job series.

6. **Special Deputation Eligibility Requirements:**

- a. **Federal, State, Local and Tribal Law Enforcement Employees:** These applicants are employed by agencies that have Full-Time Statutory Law Enforcement Authority with general arrest authority. This category also includes Civilian Security Officers employed on military reservations to enforce federal law.
- b. **Security Guards and Personal Protection Employees:** These applicants are employed by the United States Government or private agencies that provide security for a specific place or building; or personal protection for dignitary, government official, or other designated person. They do not have general arrest authority. Applicants must have general law enforcement experience of at least 1 year.
- c. **USMS Employees and Contract Employees:** These are full-time USMS employees, contract Court Security Officers (CSOs), and detention officers designated by the Director.

7. **Exceptions:** Only the Deputy Attorney General (DAG), Director, Deputy Director, Associate Director for Operations (ADO), Assistant Director of Administration (ADA), and Assistant Director (AD) or the Deputy Assistant Director (DAD), for TOD of the USMS can approve exceptions to this directive.
8. **Special Consideration Requests that require DOJ approval:**
  - a. **Physical Security Specialist (GS-0080):** This category includes a Federal Security Administrator as identified in United States Office of Personnel Management (OPM), *Handbook of Occupational Groups and Families, Position Classification Standards*, who has also completed the Federal Law Enforcement Training Center (FLETC), Criminal Investigative Training Program (CITP) or Basic Protective Investigative Training Program or (FLETC) approved equivalent, if seeking to provide protection to authorized officials or property.
  - b. **International Criminal Investigative Training Assistance Program (ICITAP):** Only applications received from the Director, ICITAP, will be processed. Applications must include a request letter stating the requirement for special deputation, badge, and credentials. Once the Special Deputation Unit has processed the application, Office of Security Programs (OSP)/TOD Document & Identity Security Office will be notified by email containing the request letter and approved application. Upon receipt of the approved application, OSP/TOD Document & Identity Security Office will coordinate the issue of special deputy badge and credentials through the Director, ICITAP. The process is the same for renewals.
  - c. **United States Attorneys and Assistant United States Attorneys (AUSA):** Only applications received through a representative from the Office of the Deputy Attorney General (ODAG) will be processed. If the applicant United States Attorney or AUSA requires a firearm qualification, the local USMS district office may provide the qualification upon proof that an approved firearms training course has been completed. An updated firearms qualification is required if an extension is needed. The following websites list approved firearms training courses:
    - 1) National Rifle Association (NRA) course:  
<http://www.nrainstructors.org/searchcourse.aspx>
    - 2) National Shooting Sports Foundation (NSSF): [www.nssf.org](http://www.nssf.org)

**E. Procedures:**

1. **Procedures for USMS Sponsored Task Force Officers (TFOs):**
  - a. All TFOs with an executed agency Memorandum Of Understanding (MOU) should be specially deputized. Each TFO applicant seeking deputation must follow the deputation procedures below. Quick reference can be found on the USMS Intranet under Operational, TOD, OSP, Special Deputations, TFO SDU Process Chart, [http://156.9.232.31/da/tod/docs/process\\_chart.pdf](http://156.9.232.31/da/tod/docs/process_chart.pdf).
  - b. Special Deputy state and local officers assigned to a USMS district task force or a Regional Fugitive Task Force who require full-time unescorted access to USMS space or systems are required to undergo a background investigation to comply with [Homeland Security Presidential Directive 12 \(HSPD 12\)](#). All background investigation requests must be sent to the Personnel Security

Branch (PSB), [PSB-Contractor@usdoj.gov](mailto:PSB-Contractor@usdoj.gov). (The background investigation must be completed prior to the submission of initial application for Special Deputation). Specific procedures, to include the type of background investigation, are included in Policy Directive 17.6, [Security Programs Manager](#). The background investigation will be conducted through the USMS PSB via OPM.

- c. Officers assigned to a task force on a part-time basis or for a period of less than 1 year may be granted escorted access to USMS space in accordance with existing visitor procedures. It is the responsibility of the United States Marshal (USM), Chief Deputy United States Marshal (CDUSM), Chief Commander, or Warrant Supervisor to ensure that all Special Deputy United States Marshals without a successfully completed background investigation are escorted at all times while in USMS space. Special Deputies who do not have a successfully completed background investigation are not authorized access to USMS systems.
- d. **TFOs Badge and Credentials:** A badge and credential will only be issued for applicants who:
  - 1) Have successfully completed background investigation completed by OSP, PSB, TOD.
  - 2) Have Form [USM-3A](#), approved by SDU, OSP, TOD.
  - 3) Have committed to a 1-year minimum term of service as a member of the task force.
  - 4) Have submitted an application for a badge and credential to OSP, Document and Identity Security Office, TOD, which includes:
    - a) Two passport photos (business attire required).
    - b) Copy of approved PSB memorandum.
    - c) Copy of Form [USM-3B](#).
    - d) Completed and signed Form [USM-287](#), *Request for Badge & Credential Action*.
    - e) Signed copy of Form [USM-288](#), *Hand Receipt (Badge & Credentials)*.
- e. Full-time TFOs with an executed MOU assigned to a USMS district or Regional Fugitive Task Force may receive USMS Task Force Credentials.
- f. Special deputation for TFOs is valid for 2 years from the date of approval. If special deputation is needed for a longer period of time, a request for renewal must be submitted 60 days prior to expiration.
- g. Upon the TFO's separation, the Task Force Commander is responsible for completing Form [USM-199](#), *Separation Checklist*, and retrieving Form [USM-3B](#), from the TFO. The collected articles and a copy of Form [USM-199](#) must be sent via FedEx to: Tactical Operations Division, Office of Security Programs, 2604

Jefferson Davis Highway, Alexandria, Virginia 22301, Attn: Document and Identity Security Office.

2. **Procedures for Other Sponsoring Agencies:**

- a. **Sponsoring Agency:** The Chief administrator of the sponsoring agency has the following responsibilities:
- 1) Submits the initial and renewal requests for deputation by providing supporting documentation and a completed Form [USM-3A](#), for each applicant.
  - 2) Verifies that the applicant meets all qualification requirements.
  - 3) Provides the applicant with a copy of the Deadly Force policy from the sponsoring agency or the DOJ.
  - 4) Notifies the SDU immediately if the special deputy is charged with a criminal offense, abuse of special deputation authority, or misuse of a firearm. In addition, when a special deputy is no longer employed or assigned, or no longer requires special deputation, the Chief administrator will conduct the following:
    - a) Notify the OSP, SDU, or PSB.
    - b) Return the Badge and Credentials via Federal Express (FedEx) to TOD, OSP, Document and Identity Security Office
    - c) Email Form [USM-3B](#), to the SDU: [Spec.Dep@usdoj.gov](mailto:Spec.Dep@usdoj.gov).

3. **Application Process:**

- a. **Individual Application:** Each applicant seeking special deputation must complete a Form [USM-3A](#).
- b. **Supporting Documentation:**
- 1) Each applicant must submit an approval letter from his/her respective law enforcement agency that indicates the applicant's employer supports the special deputation. The letter must state that the applicant is not involved in any internal investigation or disciplinary action and has no Lautenberg Amendment Violations.
  - 2) Any other information requested by the SDU (i.e., Firearm qualification, Certification of completed firearm's course of instruction, Certification of Protective Investigation Training, Executive Office for the United State Attorneys (EOUSA) Affidavit, Approval Memorandum from EOUSA Assistant Director, Approval Letter from the ODAG, Endorsement Letter from AUSA, Approval Letter from Special Operations Group (SOG) Commander, Approval Letter from the AD, TOD.



4. **Expiration Date:** The expiration date for special deputation is specified on Form [USM-3B](#), and on the Credentials. Special deputations can be authorized for 1, 2, or 3 years depending on the category of the deputation. The list below indicates the time period for various deputations.
- a. **One-year Authorizations:**
    - 1) United States Attorney Task Force
    - 2) Assistant United States Attorneys (AUSA)
    - 3) Organized Crime Drug Enforcement Task Force (OCDETF)
  - b. **Two-year Authorizations:**
    - 1) Federal task forces
    - 2) USMS task forces
  - c. **Three-year Authorizations:**
    - 1) Security Guards and personal protection employees
    - 2) Inspector General (IG) special agents
    - 3) USMS special employees
- NOTE:** To avoid disruption of special deputation status, renewal requests should be submitted within 60 days of the expiration date. If the request is received (60) days after the expiration date, the individual will need to have the Oath of Office re-administered.
5. **Submission:** The sponsoring agency must submit Form [USM-3A](#), and supporting documentation via email to [spec.dep@usdoj.gov](mailto:spec.dep@usdoj.gov)
6. **Approval Process:**
- a. The Chief of the SDU, TOD, or designee, must approve all deputations for USMS employees, contract employees, and law enforcement officers, specifically those supporting the USMS mission.
  - b. **Other Sponsoring Agencies:** Requests for special deputation to support non-USMS missions require the approval of the ODAG. The steps of the approval process are:
    - 1) The SDU reviews the agency's request and applications for special deputation. Incomplete applications are returned.
    - 2) The AD, TOD, submits a recommendation to the ODAG.
    - 3) The ODAG directs the USMS as to whether or not to grant the special deputation request.
  - c. **United States Attorneys and AUSA:** Applicants may request special deputation only for the purpose of carrying firearms for personal

protection. Applications are to be submitted to the EOUSA, not the SDU. When requested by the EOUSA, the USMS will certify that each applicant has met firearm qualification standards with an approved weapon. After certification, the EOUSA sends the application to the DAG for determination. Once a determination has been made, the application is sent to the USMS for processing.

- 1) Each applicant must complete an approved 40 hour weapons handling course and provide proof of successful completion. The following websites list approved firearms training courses:
    - a) National Rifle Association (NRA) courses: <http://www.nrainstructors.org/searchcourse.aspx>
    - b) National Shooting Sports Foundation (NSSF): [www.nssf.org](http://www.nssf.org)
  - 2) USMS district offices should not make any recommendations regarding the application or provide a threat assessment. The Judicial Security Division (JSD) provides a threat history to the EOUSA, if requested.
  - 3) The USMS, as a courtesy, may qualify the AUSA on their approved course of fire. The minimum qualification score is 210.
- d. **DAG:** The DAG, in accordance with a December 1999 memorandum signed by Nicholas M. Gess, Associate Deputy Attorney General, has complete authority for several categories of deputations.

**Categories reserved for the DAG's Approval:**

- 1) **Category 2:** Where the deputation is sought for the purpose of providing protective services, i.e., An IG special agent who is a member of the protective detail of the Cabinet official.
- 2) **Category 3:** Where the deputation is sought for a law enforcement officer by a United States Attorney. In which case, the application should be submitted with the approval of the EOUSA.
- 3) **Category 4:** Where the deputation is sought for the purpose of providing extraterritorial law enforcement authority. In which case, the application should be submitted with the approval of the affected agencies and components.
- 4) **Category 5:** Where the deputation is sought for a federal employee who does not have other federal law enforcement authority, such as an AUSA or an IG Special Agent.
- 5) **Category 6:** Where the deputation is sought for the purpose of reviewing tax information under [Title 26](#), in which case the application should be submitted with the concurrence of the Tax Division.
- 6) **Category 7:** Where the Director of the USMS determines that the request is sufficiently controversial or subject to sufficient policy concerns that it should be reviewed by a higher authority.

- e. **Group Deputations:** May be administered for special operations or events where a large group of applicants require special deputation. In these cases, the Form [USM-3C](#), *Application for Group Special Deputation*, may be used. In emergency circumstances, group deputations may take place using an abbreviated administrative process. The request letter and individual applications are waived and the applicants are listed on a consolidated log that includes name; social security number; date of birth; driver's license number; firearms qualification date; firearms make, model and caliber; and applicant's signature. After submitting the log, the agency certifies, by signature, that each applicant has met all the requirements. Form [USM-3C](#) is available online.
7. **Special Deputation Appointment:**
- a. **USM-3B:** The SDU issues Form [USM-3B](#) to the sponsoring agency prior to appointment.
  - b. **Records:** The sponsoring agency is responsible for delivering the appointee his/her deputation appointment. The original Form [USM-3B](#) is provided to the appointee. The sponsoring agency/district keeps a copy and one is emailed to SDU, OSP, TOD, at: [spec.dep@usdoj.gov](mailto:spec.dep@usdoj.gov).
8. **Oath of Office:**
- a. **Authorized Official:** Any operational employee with the rank of Assistant Chief or above is authorized to administer the Oath of Office. This responsibility may be delegated only in the absence of the aforementioned officials.
  - b. **Oath of Office:** After Form [USM-3B](#) is administered by an authorized official, a copy of Form [USM-3B](#) must be returned to the SDU for final processing.
  - c. If the individual is not deputized, a copy of Form [USM-3B](#) is returned to the SDU via email to [spec.dep@usdoj.gov](mailto:spec.dep@usdoj.gov) indicating why the individual was not deputized. Anyone not deputized within 45 days of receiving Form [USM-3B](#) must reapply.
9. **Identification and Credentials:**
- a. **Identification:** The Form [USM-3B](#) has dual purposes. It serves as the authorization for USMS districts to issue the deputation and it also serves as the appointment document that identifies that an individual is a Special Deputy. The sponsoring agency is required to issue agency credentials and/or badges. Except as otherwise provided, the USMS may issue additional credentials or badges only to specially deputized USMS employees, TFOs, and contractors.
  - b. **USMS Task Force Credentials:** At the discretion of the AD or designee, TOD, Special Deputy United States Marshals serving on USMS task forces with an executed MOU may be issued unique credentials and/or badges. Specific procedures are included in USMS directive:

**F. Responsibilities:**

1. **DAG:** Approves several categories of initial requests for special deputation except those for USMS personnel, contract employees or law enforcement officers specifically supporting USMS missions (i.e., fugitive task force).
2. **Authorized Official:** Administers the Oath of Office to applicants approved by the SDU. The authorized official completes Form [USM-3B](#) obtains the necessary signatures.
3. **AD, TOD:** Oversees the Special Deputation Program with the assistance of the DAD.
4. **Chief, OSP:** Oversees the Special Deputation Program and conducts periodic audits of the program.
5. **Chief, SDU:** Approves deputations for USMS employees, contract employees and law enforcement officers directly supporting USMS missions. This official also approves renewals for candidates previously approved by the DAG.
6. **SDU:** Processes all requests for special deputation under the direction of the Chief, SDU.

**G. Definitions:**

1. **Special Deputation:** Approved by DOJ and conferred by the USMS, it grants an individual authority to perform federal law enforcement functions to support USMS missions or to achieve law enforcement objectives.
2. **Authorized Official:** A person authorized to administer the Oath of Office.

**H. Cancellation Clause:** This policy directive supersedes Policy Directive 8.14, *Special Deputation Program*.

**I. Authorization and Date of Approval:**

**By Order of:**

**Effective Date:**

/S/  
Stacia A. Hylton  
Director  
U.S. Marshals Service

9/30/11



## United States Marshals Service POLICY DIRECTIVES

### TACTICAL OPERATIONS

#### 17.12 SECURE TELEPHONE/FAX COMMUNICATIONS

- A. Proponent:** Assistant Director, Tactical Operations Division (TOD), Office of Security Programs (OSP), United States Marshals Service (USMS) Communications Security (COMSEC) Manager, (202) 307-9390.
- B. Purpose:** To provide policy and procedures to all elements of the United States Marshals Service (USMS) relative to the Secure Telephone / Facsimile (FAX) Program.
- C. Authority:** National Policy on Securing Voice Communications [National Security Telecommunications and Information Systems Security Policy \(NSTISSP\) Nr. 101](#) which requires civil government voice systems that carry traffic of significant intelligence value to be secured.
- D. Policy:**
1. **Modes of Operation:** The STE and other secure voice devices used by the USMS are capable of operating in either the clear or secure mode. It is USMS policy that the systems be used in the secure mode when discussing classified or certain types of sensitive information as defined below.
    - a. **Classified Information:** Information that has been determined pursuant to [Executive Order 12958](#) or any predecessor Order, or by the [Atomic Energy Act of 1954](#), as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status. This information is typically identified as CONFIDENTIAL, SECRET, or TOP SECRET.
    - b. **Sensitive Information Requiring Additional Security:** Information, the loss, misuse, or unauthorized access to or modification of, which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under [5 USC 552a](#) (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
  2. **Authorized Users:** The Director, Deputy Director (DD), Associate Director for Operations (ADO), Associate Director for Administration (ADA), Assistant Directors (ADs), United States Marshals (USMs) and division chiefs, as appropriate, will make the determinations relative to authorized users. For one-time or short-term users, the local facility supervisor will limit access and follow the procedures outlined in USMS policy.
  3. **User Clearances:** All authorized users of the system must have a security clearance equal to the security level of the key contained in the secure voice device. When using

the system for classified or sensitive compartmented information, the user has the responsibility to determine that the person called has the appropriate clearances or access approvals and must be certain of that person's identity. If the STE or other secure voice device is to be used by a person without a proper clearance, the call must be placed by, and the device key controlled by, the authorized user, who will identify the individual to the called party and stipulate the classification limits of the call.

## E. Physical Security Requirements

1. **Secure Terminal Equipment (STE):** The STE is the new generation of secure voice and data equipment designated for use on advanced digital communications networks, such as Integrated Services Digital Network (ISDN). The STE consists of a host terminal and removable security core. The host terminal provides the application hardware and software. The security core is the KSV-21 cryptographic card that provides all the security services.
  - a. **STE:** The STE is a high-dollar-value item and must be protected in a manner sufficient to prevent loss and tampering. In order to prevent possible unauthorized use, a STE with a cryptographic card inserted may not be left unattended. However, the STE may be left unattended when a cryptographic card is not inserted.
  - b. **KSV-21:** This card contains cryptography and is accounted for within the COMSEC Material Control System by its unique serial number. A KSV-21 card can only be issued to a properly cleared user who possesses a clearance level equal to or greater than the keying material on the card. Once associated to a STE, the KSV-21 Fill Card becomes unclassified and is turned into a user card. A user card is UNCLASSIFIED but must be protected by being either in the user's personal possession or stored in a manner that will minimize the possibility of loss, unauthorized use, substitution, tampering or breakage.
  - c. **Loss of KSV-21 Card:** The loss of a card that has already been associated with the STE, a user card, is not a COMSEC incident. However, users are required to promptly notify the COMSEC Manager when a user card is lost so that its association with the STE can be removed at the earliest opportunity in order to prevent unauthorized access to the STE. Additionally, the COMSEC Manager must report the loss of the card through COMSEC channels and remove it from the inventory of COMSEC accountable items.
  - d. **KSV-21 Disposition:** If for any reason the KSV-21 card becomes inoperable, it must be returned to the COMSEC Manager. A user card can be transported without written courier authorization. In general, a user can send the KSV-21 card through X-ray machines or other security devices commonly used at the airport without harmful effects to the card.
  - e. **Accountability:** Each card will be accounted for using Form [SF-153](#), *COMSEC Material Report*. Each user is solely responsible for safeguarding the card and cannot further transfer the card without the knowledge of the COMSEC Manager. A user may allow or permit other people to use his or her card as long as the person is cleared to the security level of the keys programmed on the card.

2. **Special Issue COMSEC Equipment:** The USMS may deploy other voice and data COMSEC devices on a limited basis. In such cases, the USMS COMSEC Manager will ensure that users are provided with written policy guidance and verbal instruction on the use, storage, and accountability requirements of the specific device in accordance with the relevant National Security Agency (NSA) and Department of Justice (DOJ) policies.
3. **Secure Facsimile Transceivers:** Secure Facsimile machines are currently operating in conjunction with STE telephones, providing secure data capabilities throughout the USMS. A limited number of machines are also available for short-term use during a USMS field operation. Additional terminals can be purchased locally after consultation with the COMSEC Manager. The COMSEC Manager will identify specific machines which may be purchased in order to ensure compatibility and interoperability with existing equipment.
- F. **Definitions:** Refer to [12-4 Appendix 1](#) for definitions.
- G. **Cancellation Clause:** Supersedes Policy Directive 12.4, *Telecommunication: Secure Telephone / FAX Communications*.
- H. **Authorization Date and Approval:**

**By Order of:**

/S/  
John F. Clark  
Director  
U.S. Marshals Service

**Effective Date:**

6-15-2010



## United States Marshals Service POLICY DIRECTIVES

### TACTICAL OPERATIONS

#### 17.13 SPECIAL OPERATIONS GROUP

- A. Proponent:** Commander, Special Operations Group (SOG), Phone: 318-640-4560, Fax: 318-640-7094.
- B. Purpose:** This policy directive contains policy and procedures for requesting tactical support and deployment of the United States Marshals Service (USMS) SOG.
- C. Authority:** The Director's authority to issue written directives is set forth in [28 U.S.C. § 566](#).
- D. Policy:** SOG is a specially trained and equipped unit deployed for high-risk/sensitive law enforcement situations, national emergencies, civil disorders, and natural disasters to support USMS districts and headquarters divisions.
1. SOG is authorized to deploy and use (b) (7)(E) not mentioned in Policy Directive 2.3, [Firearms](#) or Policy Directive 2.1, [Less Than Lethal Devices](#). The Assistant Director (AD), Tactical Operations Division (TOD), and the SOG command staff will specify which (b) (7)(E)  
    - a. (b) (7)(E)
    - b. To satisfy mission requirements, SOG may procure weapons, ammunition, and ordnance (b) (7)(E)
    - c. SOG may procure ammunition (b) (7)(E)
    - d. SOG armorers are authorized (b) (7)(E)
  2. SOG personnel will maintain custody of their SOG issued firearms to allow for in-district training and qualifications and to enhance operational readiness.



- a. SOG personnel may carry either (b) (7)(E) [REDACTED]  
[REDACTED]  
[REDACTED]
- b. SOG personnel are authorized (b) (7)(E) [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]
- c. SOG personnel may deploy their (b) (7)(E) [REDACTED]  
[REDACTED]

**E. Procedures:**

**1. Requests for SOG Support:**

- a. During normal business hours, districts and divisions should submit requests for SOG tactical support on a Form [USM-535](#), *Request for Special Assignments Resources*, to the SOG Commander. During non-business hours, requests should be sent to the USMS Communications Center, which will immediately contact the AD, TOD.
- b. Requests for SOG support will be made as far in advance of the mission as possible to allow for thorough tactical assessment and planning. During exceptional situations, or situations that require an immediate response, the district or division may contact the SOG Commander directly, who will then advise the AD, TOD. Upon receiving oral approval of the request from the AD, TOD, the SOG Commander will contact the district or division. The requestor must still submit a Form [USM-535](#) as soon as possible.
- c. SOG will review each request to determine staffing and equipment requirements and then send the request to the AD, TOD, for approval.

**2. Deployment of SOG:**

- a. After the Form [USM-535](#) is approved, the SOG Commander will deploy SOG members by the most expedient means available; and
- b. Travel will be scheduled for the first available departure date consistent with the SOG operational plan. SOG members will be permitted to make travel arrangements using their assigned government travel cards. SOG will prepare a Deployment Authorization e-mail and send it directly to the affected district(s).

**3. Coordination and Cooperation:**

- a. SOG direct chain of command is through the AD, TOD. During each deployment, the SOG Commander or designee will direct SOG personnel, logistics, and assets.
- b. (b) (7)(E) [REDACTED]  
[REDACTED]  
[REDACTED]

- c. Once SOG has permission to commit its resources to a district operation, the SOG Commander will communicate directly with the appropriate United States Marshal (USM). The SOG Commander will ensure that the USM, Chief Deputy United States Marshal (CDUSM), and the AD, TOD, are informed or consulted as necessary on significant events or tactical decisions; however, tactical command and authority over the mission remain with the SOG Commander or designee.

**4. District Support Requirements:**

- a. Districts that have active SOG members are required to support SOG missions and training by deploying those personnel when requested by the SOG Commander.
- b. SOG maintains an operational rotation schedule consistent with unit organization. SOG makes every effort to deploy personnel consistent with the schedule; however, circumstances such as large scale deployment, or the need for specialty or leadership positions, may require SOG to deploy personnel outside of the rotation schedule. The SOG operational rotation schedule is provided annually to affected district managers.

**5. Specialized Capabilities:**

- a. (b) (7)(E) [REDACTED]
- b. (b) (7)(E) [REDACTED]
- c. (b) (7)(E) [REDACTED]
- d. (b) (7)(E) [REDACTED]
- e. (b) (7)(E) [REDACTED]
- f. (b) (7)(E) [REDACTED]
- g. (b) (7)(E) [REDACTED] and [REDACTED]
- h. (b) (7)(E) [REDACTED]

**F. Responsibilities:**

- 1. AD, TOD: Has management and oversight responsibility of SOG. In concert with the Associate Director for Operations (ADO) and the Office of the Director, gives final approval of requests for tactical support, authorizes deployment of, and has operational control over SOG.

2. **SOG Commander:** Advises SOG and the AD, TOD, on all matters concerning tactical operations and deployment of SOG and oversees SOG activities during operations. Serves as the headquarters point of contact for deployment of SOG. Has operational control of SOG during tactical operations and advises the AD, TOD, ADO, and the Office of the Director on all matters concerning tactical operations and deployment of SOG and oversees SOG activities during tactical operations. Ensures that all necessary training for SOG members is provided; monitors and evaluates SOG; and maintains necessary records.
3. **SOG Deputy Commander:** Serves as the Acting SOG Commander when the SOG Commander is unavailable. Assists with the above requirements as directed.
4. **Districts:** Ensure that personnel assigned to SOG are available for immediate deployment.

**G. Definitions:**

1. **Tactical Support:** SOG personnel with specialized training and equipment within an organized team structure.
2. **Emergency Situations:** Tactical support required within 24 to 72 hours of an initial request.
3. **Exceptional Situations:** Those requiring immediate deployment of SOG.
4. **SOG Personnel:** Includes current full time and current collateral duty SOG qualified operational personnel.

**H. Cancellation:** Supersedes USMS Policy Directive 2.4, *Operations Support: Special Operations Group*.

**I. Authorization and Date of Approval:**

**By Order of:**

**Effective Date:**

/S/

4-21-2010

John F. Clark  
Director  
U.S. Marshals Service



# United States Marshals Service **POLICY DIRECTIVES**

## **TACTICAL OPERATIONS**

### **17.14 OPERATIONAL MEDICAL SUPPORT UNIT**

- A. Proponent:** Medical Program Manager (MPM), Special Operations Group (SOG), Tactical Operations Division (TOD). Telephone: 318-640-4560, Fax: 318-640-7094.
- B. Purpose:** This policy directive sets forth direction for the establishment and use of the United States Marshals Service (USMS) Operational Medical Support Unit (OMSU). This policy provides guidance relating to emergency medical care and a safe working environment for all USMS employees, protectees, and other law enforcement personnel assisting Deputy United States Marshal (DUSM) Medics.
- C. Authority:** The Director's authority to issue policy directives is set forth in [28 U.S.C. § 566](#).

In 1966, the [National Highway Safety Act](#) appointed the United States Department of Transportation (USDOT) as the agency responsible for developing Emergency Medical Service (EMS) standards throughout the United States. In 1970, the National Registry of Emergency Medical Technicians (NREMT) was founded to establish professional standards and provide services to local EMS providers. The standards established by the NREMT, along with a detailed volume of medical protocols, serve as the framework for the USMS OMSU.

#### **D. Policy:**

1. Supervision and guidance of medical care rendered by DUSM Medics shall be by an OMSU Medical Director, who is a licensed physician and approved by the Assistant Director (AD), TOD. Supervision and guidance will be accomplished through the following two methods:
  - a. **Online Medical Control:** When the DUSM Medic is receiving orders from the OMSU Medical Director or designee onsite or through other means of communications.
  - b. **Offline Medical Control:** When the DUSM Medic is functioning in accordance with established patient care protocols as approved by the OMSU Medical Director.
2. DUSM Medics shall:
  - a. Initiate immediate emergency medical care to stabilize injuries and/or preserve life during USMS law enforcement operations when physically present. This will provide a resource for the immediate initiation of emergency medical treatment at an injury site. This care bridges the gap between the time and place of injury and the subsequent arrival of civilian EMS providers. This is particularly important during missions which, due to ongoing law enforcement operations, will not permit civilian EMS providers within the immediate area.
  - b. Follow the medical protocols set forth by the OMSU Medical Director.

- c. Reasonably anticipate and minimize the risk of injuries during USMS law enforcement operations by completing Form [USM-462](#), *OMSU Medical Threat Assessment* (MTA), prior to OMSU-involved operations.
- d. Provide medical support and monitor the health of personnel during high-risk USMS operations and training events.
- e. Provide education and training in current tactical medicine standards of care.

**E. Responsibilities:**

1. **AD, TOD:** Provides overall administration and management of the Medical Support Program.
2. **Commander, SOG:** Provides oversight of program execution. Reports program processes and issues to the AD, TOD.
3. **OMSU Medical Director:**
  - a. Maintains Emergency Medical licensure under which all OMSU Medics are certified.
  - b. Establishes standard medical protocols and practices.
  - c. Provides a recertification course that adheres to the minimum standards of the NREMT.
4. **Medical Program Manager (MPM):**
  - a. Identifies and coordinates available medical resources to include review of operational plans/orders as requested by district/division management and maintains a roster of qualified DUSM Medic personnel to ensure proper support of high-risk operations.
  - b. Coordinates the development and implementation of the Emergency Medical Technician (EMT) training program and maintains training records.
  - c. Selects appropriate medical equipment for issuance.
  - d. Selects appropriate medical equipment for operations and facilitates DUSM Medics' access to specified equipment.
  - e. Develops and oversees the Quality Assurance Program as it pertains to patient care reports and program progress. Provides a status report to the SOG Commander on a monthly basis; the status report will include, but not be limited to, a summary of patient care provided, obligation of funds, training attended, OMSU deployments, and any other significant events.
5. **Senior Medic:**
  - a. Ensures that DUSM Medics in his or her respective region are maintaining the Patient Care/Clinical Hour requirement; maintains a monthly log and verifies that hours are completed by providing quality checks at his/her discretion with the reported provider through which the DUSM Medic is achieving his or her hours. The monthly log will be submitted to the MPM no later than the fifth business day of each month and will contain, at minimum, the following:

- 1) The date hours were performed;
  - 2) The number of hours performed;
  - 3) The hospital/clinic or EMS service where hours were performed; and
  - 4) The name and phone number of the supervisor or lead medic who can verify the number of hours performed and the number of patients with which the DUSM Medic had contact.
- b. Ensures that the DUSM Medic has submitted a MTA and reported his/her involvement prior to OMSU supported events or operations. Reviews the accuracy and completeness of each MTA prior to submission to the MPM. MTAs will be submitted to the MPM prior to an OMSU supported event. Exceptions to this will be limited and on a case-by-case basis.
  - c. Ensures that Patient Care Reports (PCRs) are compiled and submitted for each medical incident where treatment was rendered by a DUSM Medic to an injured person. The Senior Medic reviews the PCR for accuracy and completeness. Where follow up is needed, the Senior Medic will provide clarification to the DUSM Medic. The Senior Medic then forwards the finalized PCR to the MPM.
  - d. Ensures an accurate log is kept for each DUSM Medic to reflect the DUSM Medic's training and operational commitments. Logs are submitted to the MPM on a monthly basis.
6. **DUSM Medics:**
- a. Provide medical support for USMS operations. All DUSM Medics are required to support nationwide operations.
  - b. Provide emergency care of seriously ill or injured USMS personnel, the judiciary, United States Attorneys, suspects, fugitives, and bystanders, and document any treatment rendered with a PCR. The PCR is sent to the Senior Medic by way of email correspondence.
  - c. Prepare MTAs for OMSU-supported law enforcement and protective operations. Prior to the start of an OMSU-supported operation, DUSM Medics are to provide an MTA to their Senior Medic and the Supervisory Deputy United States Marshal (SDUSM) in charge of the operation by way of email correspondence.
  - d. Maintain awareness and compliance with all pertinent medical treatment protocols and standing orders as defined by the OMSU Medical Director.
  - e. Ensure that Patient Care/Clinical Hour requirements and continuing education training recertification criteria are met to maintain EMT certification. Documentation is forwarded to the Senior Medic to monitor fulfillment of continuing education requirements.

**F. Procedures:**

1. **Medical Response Levels:** The USMS OMSU is based on medical support response at the following three levels:


- a. **DUSM Medic:** A DUSM who has attained the state or national certification equivalent or higher to the NREMT at the EMT or EMT-Basic level. All DUSM Medics will attend the OMSU Medical Director's training once every 2 years to receive their Expanded Scope Protocols Training and Certification.
  - b. **DUSM Paramedic:** A DUSM who has attained the state or national certification equivalent or higher to the NREMT at the EMT Paramedic equivalent or higher level.
  - c. **Medical Support Team:** If it is determined that an operation requires a higher level of medical support than described above, the MPM may request a Medical Support Team be deployed to support the USMS operation. These teams will be used in accordance with USMS procedures. The Medical Support Team consists of the OMSU Medical Director and/or his/her designee(s).
2. **Medic Deployment:** The use of DUSM Medics will be considered (b) (7)(E) [REDACTED]
- [REDACTED] The appropriate manager, district/division Supervisor, Inspector, or higher, will be responsible for requesting operational medical support. Unless prohibited by circumstances (i.e., Operational Security (OPSEC) concerns), DUSM Medics should not be used as replacements for civilian EMS providers during operations. The function of DUSM Medics and Medical Support Team personnel is to provide immediate onsite care during USMS operations that preclude the use of civilian EMS providers. Such situations may include but are not limited to the following:
- a. (b) (7)(E) [REDACTED]
  - b. (b) (7)(E) [REDACTED]
  - c. (b) (7)(E) [REDACTED]
  - d. (b) (7)(E) [REDACTED]
  - e. (b) (7)(E) [REDACTED] and
  - f. (b) (7)(E) [REDACTED]

3. **Procedures for Requesting Medical Support:**


- a. DUSM Medics may be utilized within their district/division at the discretion of the respective United States Marshal, Chief Deputy United States Marshal, or AD. District/division management may request support from OMSU, as necessary, to determine and meet operational requirements.
- b. Funding for such operations will be drawn either from district funds or special assignment funding, as approved through the normal special assignment authorization process detailed in USMS Policy Directive 2.4, [Special Assignments](#). OMSU does not fund nor reimburse losing or gaining districts/divisions utilizing OMSU DUSM Medics with regards to travel, MIE, or other miscellaneous costs associated with the operation.
- c. OMSU does not fund or reimburse districts/divisions for guard hire.
- d. OMSU does not fund or reimburse districts/divisions for overtime incurred while on OMSU-endorsed operations or training.

- e. Requests for DUSM Medics can be made to the region's OMSU Senior Medic where the operational need for OMSU support is occurring. Through the Senior Medic, OMSU will provide the roster of DUSM Medics who are in good standing within OMSU at that particular time to the requesting district/division. The OMSU Senior Medic will notify the MPM at the SOG Tactical Center of the pending operation and the deployment of the particular OMSU medic. The Senior Medic also may contact the MPM if medics in the region are unable to support the request. The MPM will reach out to adjacent regions through the Senior Medics to solicit further assistance. It remains the responsibility of the requesting district/division to further coordinate with the supporting OMSU Medic's district/division management. District/division management must notify OMSU when DUSM MTA Medics are utilized for special assignments.

4. **Medical Threat Assessment (MTA):**

- a. (b) (7)(E)  

- b. The MTA is part of the overall operations plan.
- c. Once deployed, DUSM Medics will document any considerable change from their recommendations or pre-operational planning on the MTA.
- d. DUSM Medics will be aware of operational security concerns when completing MTAs and should coordinate such activity with the operational supervisor in charge.
- e. Completed MTAs will be forwarded via email to the respective Senior Medic for review prior to OMSU-supported operations. MTAs will also be given to the Operational Supervisor in charge of the operation prior to the start of an OMSU-supported operation. The Senior Medic will review and forward MTAs via email to the MPM. MTAs will be maintained to provide a resource to DUSM Medics for future operations.
- f. The MTA should have a minimum classification of Unclassified//Law Enforcement Sensitive (U//LES).

5. **Medic Procedures:**

- a. DUSM Medics will make recommendations to the on-scene commander regarding medical concerns before and during an operation.
- b. (b) (7)(E)  

- c. DUSM Medics will administer medical care in accordance with USMS-approved protocols.



- d. DUSM Medics provide a wide-range of preventive care, which may include, but is not limited to, dispensing over-the-counter medication, bone/joint care, and hydration. DUSM Medics will use operational funding for additional items required during an operation for preventive care and replenishing items utilized while performing care during an operation.
- e. DUSM Medics should contact the OMSU Medical Director or designee while on an operation if the need for further consultation or medical guidance arises. The consultation may guide further treatment, referrals, or other patient care decision making options.
- f. DUSM Medics will forward PCRs to their respective Senior Medic via email for review. The Senior Medic will then forward to the MPM as soon as practical following emergency care.
- g. DUSM Medics will use universal precautions as outlined in the [USMS Bloodborne Pathogen Program](#).
- h. DUSM Medics will refer to USMS Policy Directive 9.32, [Death of Federal Prisoners](#), for proper reporting requirements and USMS Policy Directive 9.04, [Prisoner Health Care](#), for prisoner healthcare provisions while in custody.

**6. Operational Environment Triage:**

- a. Triage protocols will be instituted when operations result in more than one person sustaining injuries.
- b. When medically appropriate and operationally necessary, injured law enforcement officers will receive priority perfunctory care to return them to the operative mission.
- c. Medical treatment of protected persons will be deemed a priority once the environment has been deemed safe.
- d. Medical treatment of injured persons under USMS control, including suspects, should not be accomplished until it can be determined that those persons are no longer a threat.

**7. Patient Transportation:**

- a. DUSM Medics will anticipate the possibility of transporting seriously ill or injured persons on every operation. As part of pre-operational planning, DUSM Medics should be familiar with the following:
  - 1) Procedures for requesting and notifying civilian EMS providers. OPSEC will always be a concern of the DUSM Medic when interacting with civilian EMS.
  - 2) Routes to trauma hospitals and specialty hospitals if the need for immediate transportation outweighs waiting for a local civilian EMS transport.
  - 3) Procedures for requesting helicopter medical evacuation for seriously injured persons, especially if ground transportation to a trauma center

would be excessive or difficult. DUSM Medics will plan the location and identify landing zones as necessary.

- 4) Procedures for handcuffing injured prisoners.
  - b. DUSM Medics will ensure that injured prisoners in USMS custody requiring transportation to medical facilities by civilian EMS providers are accompanied in the transporting vehicle by (b) (7)(E) DUSM and that established USMS procedures relating to custody of suspects are followed.
8. **Selection of Medics:** All prospective DUSM Medics will be nationally certified with the NREMT at the EMT or EMT-Basic level at a minimum. OMSU does not fund the initial EMT or EMT-Basic Certification training.
- a. Selection of DUSMs who are currently certified at the NREMT equivalent EMT or EMT-Basic level will comply with the following:
    - 1) Complete Form [USM-461](#), *Operational Medical Support Unit Application*, with the appropriate management endorsements and submit to the MPM.
    - 2) Attach copies of current NREMT certification and current Cardio-Pulmonary Resuscitation (CPR)-Healthcare provider certification to the request.
    - 3) Provide a signed OMSU Provider Disclosure Statement.
  - b. Final selection of DUSM Medics will be made in consultation with the respective region's Senior Medic, MPM, and the OMSU Medical Director.
  - c. No DUSM shall operate as a DUSM Medic under OMSU without the approval of the OMSU Medical Director and MPM. DUSMs selected to participate in OMSU shall follow all directions and guidance provided by the OMSU Medical Director.
  - d. DUSM Medics support a wide variety of USMS programs and possess unique expertise. DUSM Medics may support SOG operations even though they are not SOG members. During SOG operations, DUSM Medics will be subject to the command and control of the SOG Supervisor and the SOG Medic.
9. **Removal of DUSM Medics:**
- a. OMSU is a voluntary program. DUSM Medics may resign via written submission to the MPM.
  - b. DUSM Medics may be removed from the OMSU based on quality concerns. The MPM and OMSU Medical Director will initially attempt to correct any care issues through training and counseling. If the situation is not resolved through remediation, the MPM will remove the DUSM Medic from the program.
  - c. The MPM will monitor DUSM Medics via a combination of operational reporting, such as through PCR/MTA submissions, field evaluations, and through advisement from their respective Senior Medic. The MPM or Senior Medic will provide feedback to a DUSM Medic who is deficient in one or more areas in an attempt to correct the situation. Continued deficiencies may result in removal from the program.

- d. Any DUSM Medic who fails to successfully meet NREMT or state recertification standards may be removed from the program.
- e. Any DUSM Medic who fails to achieve the Patient Care/Clinical Hour requirements may be removed from the program.
- f. Any DUSM Medic may be removed at any time for not adhering to OMSU policy.

10. **Training:**

- a. **Documentation:** To ensure that USMS DUSM Medics are trained and certified to provide effective emergency medical care, the following minimum training requirements must be documented by the MPM: state or NREMT certification, continuing education hours, and a valid Healthcare Provider CPR card.
- b. **Patient Care/Clinical Hour Requirement:**
  - 1) Acquired hours that are essential for developing and retaining effective pre-hospital emergency care skills. Toward this end, DUSM Medics must perform a total of 24 hours of patient care every 3 months. Patient care hours are defined as performing patient care through a scheduled clinical or a local EMS setting such as, but not limited to, hospitals, clinics, fire services, ambulance services, scholastic athletic programs, the United States Military, and/or other United States Government patient care facilities. Districts are encouraged to authorize this patient care/clinical hours training to occur during normal work hours, depending on district workload. Patient care hours may also be acquired up to 8 hours every 3 months by providing actual patient care. Nonscheduled, actual patient care hours will be documented utilizing a PCR. Each PCR, up to eight individual PCRs, will account for 1 hour towards the patient care/clinical hour requirement.
  - 2) OMSU Deputy Medics are considered on official government duty when they are conducting monthly scheduled clinical hours.
- c. **EMT Recertifications:**
  - 1) Will be completed in accordance with NREMT requirements and will be verified by the OMSU Medical Director. Currently, NREMT requires recertification every 2 years, with an expiration date of March 31, on every scheduled renewal year. The OMSU will fund the recertification fees for medics in compliance with this policy directive. In accordance with these criteria, DUSM Medics must submit a copy of their new NREMT cards or state cards to the MPM or designee upon receipt from NREMT or the state governing body. This information will be maintained by OMSU.
  - 2) The OMSU will provide and fund training that meets the NREMT requirements for recertification at the EMT or EMT-Basic level. DUSM Medics with higher levels of certification must individually complete their additional required curriculum training.
- d. **CPR:**
  - 1) Certification as a CPR Healthcare Provider remains valid for a 2-year

period and is a requirement for NREMT recertification. Certifications must be sent to the MPM or designee.

- 2) The OMSU Medical Director will provide oversight and maintain medical control over DUSM Medics issued an OMSU automatic external defibrillator.
- e. **Senior Medics:** The MPM will designate certain experienced DUSM Medics as Senior Medics. These Senior Medics will conduct documentation and peer reviews of training, monthly clinical hours, PCR's, MTAs, and skills of other DUSM Medics. These peer reviews and documentations, which will in turn be reviewed by the MPM and OMSU Medical Director, will ensure compliance with established standards and protocols. Senior Medics are appointed by the OMSU MPM, in consultation with the OMSU Medical Director, and may not be designated by district/division managers.
- f. **Policy and Protocol Proficiency:** DUSM Medics must attend one OMSU recertification course every 2 years regardless of NREMT or state certification to show competency in the current OMSU Policy and Protocols. Proficiency may be demonstrated through written/oral exams or hands on applications. Deficiencies in knowledge or application of policy or protocol will be addressed and corrected. A DUSM Medic may be asked to depart the program in the event he or she is unable or unwilling to make corrections to maintain compliance.
- g. **Confidentiality:**
- 1) DUSM Medics may be provided with a person's medical history information, which may be essential in ensuring proper emergency medical treatment. Confidentiality of this information is of paramount concern for DUSM Medics, who will ensure that it is not accessible to nonmedical personnel. Additionally, DUSM Medics shall always use their best judgment when disclosing any medical information.
  - 2) DUSM Medics shall only release medical information under the following circumstances:
    - a) When such release is authorized by the employee or person providing the information;
    - b) When the medical information is released to health care providers under emergency conditions;
    - c) When the risk of not disclosing information regarding medical history or condition presents a clearly definable risk to the employee or to others involved in an operation. In this situation, the DUSM Medic will counsel the person in an effort to encourage the employee to either inform appropriate supervisory personnel of the condition or to remove the employee from the operation. If the person declines to inform appropriate supervisors of a condition that may endanger the person or others, after consultation with the MPM, the DUSM Medic will inform the appropriate supervisor of the situation. Notification of the appropriate supervisor will be done in a manner that is considerate of the person's right to privacy; or

- d) When an in-custody prisoner or new arrestee needs further medical treatment or when turning over patient care to an emergency health care entity or service.

**11. Medical Documentation:**

- a. Any emergency care provided by DUSM Medics in the course of duty shall be documented on a PCR. This documentation will clearly and accurately reflect the extent of medical treatment administered by the DUSM Medic. This documentation will also reflect the mode of transportation and the facility where the patient was taken. If the patient was turned over to a civilian EMS provider, the name of the provider and the transporting unit designation shall be documented. Patients contacted when conducting monthly clinical hours in a scheduled medical clinic setting are excluded from documentation on a PCR.
- b. Completed PCRs will be emailed to the respective Senior Medic after providing patient care. Exceptions may be made by the MPM for operational security concerns. The DUSM Medic may communicate directly with the MPM in cases with exceptions.
- c. Any DUSM Medic who performs emergency care during non-USMS activities must notify his/her respective Senior Medic after rendering care. This notification will detail the circumstances under which the care was rendered. A PCR will be utilized for documentation and sent via email to the respective Senior Medic.
- d. Upon receipt of a completed PCR, the Senior Medic will forward it via email to the MPM. The MPM will ensure that email copies are distributed to the appropriate personnel, including the OMSU Medical Director, and that these medical records are stored in a manner that is consistent with OMSU Policy.

**12. Declination or Refusal of Medical Treatment:**

- a. Consent must be obtained in order to perform pre-hospital care with any conscious and mentally stable individual. Implied consent occurs when the patient is unresponsive or considered to have impaired judgement.
- b. In a noncustodial situation where a patient refuses care or transportation, DUSM Medics will complete a PCR in its entirety, describing the extent of injuries sustained and the extent of medical treatment rendered up to the point where consent was withdrawn. Any emergency care or procedure that should have been performed in accordance with established protocols, but which the patient refused, must be documented on this form.
- c. DUSM Medics may document a refusal of care using the PCR or other means ensuring it is witnessed by another law enforcement officer or healthcare provider. Should a patient refuse to sign, the DUSM Medic will document this refusal and have a witness document the refusal with his/her signature and date.
- d. Suspects in USMS custody may refuse medical treatment, but cannot refuse transport to a medical facility if the DUSM Medic deems it necessary. A suspect in USMS custody who declines medical treatment "Against Medical Advice" will be transported to an emergency department to be evaluated by a physician. The details of the injuries sustained, along with any post-injury "Care Instructions" provided by the emergency room, must be communicated to the personnel of the holding facility where the prisoner will be housed. The DUSM Medic will

document refusal of care on the PCR. The PCR shall be completed in its entirety, describing the extent of medical treatment administered up to the point where consent was withdrawn and documenting the name of the receiving facility where the suspect was transported and evaluated.

- e. When a DUSM refuses medical treatment, the DUSM Medic shall notify the DUSM's immediate supervisor of his/her refusal and document on the PCR.
- f. PCRs must be forwarded to the Senior Medic who will review for completeness prior to sending via email to the MPM in accordance with the confidentiality procedures outlined in this policy.

13. **Bloodborne Pathogen Exposure:**

- a. Documentation of potential exposure to bloodborne pathogens will be in accordance with USMS policy including the completion of a CA-2 form.
- b. All DUSM Medics should be thoroughly familiar with and adhere to the guidelines found in USMS Policy Directive 3.5, [Exposure Control Plan for Occupational Exposure to Pathogens, Exposure to Bloodborne and Airborne \(Tuberculosis\) Pathogens](#). Refer to the [Environmental, Occupational Safety and Health Website](#) for additional guidance.

14. **Memorandum of Understanding:**

- a. A physician will serve as the OMSU Medical Director. This physician will provide medical control, which may include standing orders, medical treatment protocols, and quality improvement for DUSM Medics.
  - 1) A contractual agreement with a comprehensive statement of work should exist in writing.
- b. Medical support consists of the following:
  - 1) Consultative services prior to operations, including training, mission planning, and medical information analysis.
  - 2) Upon request, direct field medical support and extended mission support as a supplement to DUSM Medics. Personnel supplied for this support should be able to satisfy the requirement of a secret security clearance at a minimum.
- c. Quality Assurance:
  - 1) The OMSU Medical Director may review the documentation of all medical treatments rendered by DUSM Medics that occur during USMS operations. These reviews will be conducted to ensure that appropriate care was rendered and that adequate documentation of the medical treatment was performed.
  - 2) The OMSU Medical Director may recommend the removal of any DUSM Medic from the program for documented cause. The MPM will review such a recommendation.

15. **Equipment:**

- a. **Medical Equipment:** The MPM will ensure each individual DUSM Medic has sufficient basic emergency medical equipment. The OMSU Medical Director will approve this equipment for use.
- b. **Replacement Equipment:** All OMSU medications and equipment should be inspected routinely. DUSM Medics are to request medications and equipment replacement through their respective Senior Medic. OMSU medications and equipment will be replaced if financial resources are available. DUSM Medics must have prior approval from the MPM before acquiring any other medical equipment (e.g., from the Defense Reutilization and Marketing Office or hospital sources) for the administration of medical care for training purposes.
- c. **Advanced Life Support (ALS) Equipment:** DUSM Medics who have been approved by the OMSU Medical Director to perform ALS skills will be issued the appropriate equipment if financial resources are available.

**G. Definitions:**

- 1. **Advanced Life Support (ALS):** Advanced pre-hospital emergency care of the seriously ill or injured by appropriately trained and certified EMT's and EMT-Paramedics. The skills available to ALS providers include but are not limited to intravenous and drug therapy, advanced airway support, and cardiac monitoring.
- 2. **Basic Life Support (BLS):** Pre-hospital emergency care of the ill or injured by appropriately trained personnel, generally using basic skills defined in the USDOT EMT curriculum.
- 3. **CPR:** The combination of artificial respiration and circulation performed as an emergency procedure when cardiac and respiratory arrests have occurred.
- 4. **EMS:** The ALS and BLS organizations used to respond to a person requiring immediate medical care to prevent loss of life or aggravation of illness or injury.
- 5. **EMT:** An individual trained to provide pre-hospital emergency medical treatment in accordance with standards established by the USDOT. An OMSU EMT may have additional "Expanded Scope Protocols" not traditionally granted by civilian EMS organizations.
- 6. **Emergency Medical Technician-Paramedic (EMT-P):** An individual trained in accordance with USDOT standards to provide pre-hospital emergency medical treatment at an advanced life support level.
- 7. **Hospital Site Survey:** Process by which a DUSM Medic identifies and evaluates a medical facility to ascertain its capabilities and restrictions as it relates to the treatment of severely ill and injured victims.
- 8. **Medical Control:** A system that involves the medical community in all phases of the EMS system in an effort to ensure the delivery of effective pre-hospital emergency care.
- 9. **OMSU Medical Director:** Designated physician responsible for overseeing pre-hospital care providers (DUSM Medics) within the USMS OMSU Program.

10. **Medical Program Manager (MPM):** USMS SOG SDUSM assigned to supervise the USMS OMSU and interact with the OMSU Medical Director.
11. **Medical Protocols:** Written prescribed medical procedures for use by pre-hospital emergency care providers.
12. **Medical Support Team:** A physician and an independent duty paramedic deployed by a USMS approved support organization. This team is capable of rendering emergency care as well as providing short- and long-term support of the medical needs of a law enforcement mission. Also included with the Medical Support Team, but non-deployable, is the Mission Support Specialist. He or she is used to develop medical intelligence, query medical databases, and provide other administrative and consultative services to deployed Medical Support Team members.
13. **Medical Threat Assessment (MTA):** A pre-operational evaluation, prepared by the DUSM Medic of the medical needs for a USMS operation, including contingencies in case of illness or injuries.
14. **National Registry of Emergency Medical Technicians (NREMT):** An organization that establishes a national standard for certification and maintenance of EMTs at the BLS and ALS levels.
15. **Off-line Medical Control:** The oversight of pre-hospital emergency care through the issuing of OMSU Medical Director-approved protocols or standing orders that define a provider's scope of practice.
16. **On-line Medical Control:** The oversight of pre-hospital medical care by a physician onsite or through some mode of communication.
17. **Patient Care Report (PCR):** Documentation of a patient assessment; the course of a patient's condition, and treatment.
18. **Scope of Practice:** Refers to those EMS procedures that a certified person is permitted to perform or is authorized to perform, pursuant to his or her certification, by medical-command authorization or protocol.
19. **DUSM Medic:** A USMS DUSM trained and certified as an EMT or Paramedic, according to USDOT standards. He or she is recognized by the USMS as being an active participant in the USMS OMSU program.
20. **Trauma Hospital or Trauma Center:** A medical facility that is accredited by national standards and specially equipped and prepared to treat and care for trauma victims. Trauma Hospitals/Centers may be designated at different levels, depending on the capabilities of a particular hospital/center.

**H. References:** None.



**I. Cancellation:** This policy directive supersedes Policy Directive 17.14, *Medical Support Program*.

**J. Authorization and Date of Approval:**

**By Order of:**

**Effective Date:**

/S/  
Stacia A. Hylton  
Director  
U.S. Marshals Service

10/7/2013



# United States Marshals Service POLICY DIRECTIVES

## TACTICAL OPERATIONS

### 17.15 OCCUPANT EMERGENCY PROGRAM (OEP)

- A. Proponent:** Office of Security Programs (OSP), Tactical Operations Division (TOD).  
Telephone: 202-307-5129, Fax: 202-307-3446.
- B. Purpose:** This section defines the United States Marshals Service (USMS) OEP and establishes the duties and responsibilities for the formulation and implementation of the program.
- C. Authority:** The Director's authority is set forth as indicated:
1. The Director's authority to supervise the USMS is contained in [28 U.S.C. § 561 \(g\)](#), [28 C.F.R. § 0.111](#), and [Public Law 106-544](#).
  2. Department of Justice ([DOJ Order 2600.2D](#), *Security Programs and Responsibilities*, prescribes the general duties and responsibilities of Security Programs Managers (SPMs) and Security Officers, TOD, for the preparation and maintenance of effective contingency plans to ensure the protection of life and property in federally occupied space.
  3. [DOJ Order 1779.2A](#), *Occupational Safety and Health Program*, prescribes the general duties and responsibilities of Safety and Health Managers for advising SPMs of the safety and health requirements necessary for developing an OEP for the building and/or facility where DOJ is the prime tenant.
  4. [DOJ Order 2630.4C](#), *OEP*, prescribes the general duties and responsibilities for DOJ components for the formulation, coordination, and implementation of an effective OEP containing organizational and emergency response procedures required to protect life and property during the evacuation of any DOJ building and/or facility throughout the United States.
- D. Policy:**
1. USMS policy is to protect life and property by maintaining an effective OEP in each USMS building and/or facility throughout the United States.
  2. When the USMS is not the prime tenant in a building and/or facility, the United States Marshal (USM), or his/her designee, and the Security Officer cooperates with the prime tenant to establish an effective OEP. If the prime tenant fails to develop an OEP, the USM or designee must develop an OEP for the building and/or facility to ensure the safety of USMS personnel and the protection of DOJ property.
- E. Responsibilities:**
1. **SPM:** The SPM is appointed by the Director and is responsible for managing the Security Programs and coordinating the OEP with the Designated Official (DO). The SPM is also responsible for coordinating with the DO and the Occupant Emergency Organization (OEO). The SPM coordinates the OEP with the DO and ensures the preparation, implementation, and maintenance of an OEP for every building or facility occupied by USMS employees. Additionally, the SPM is responsible for oversight of the

selection, organization, and training of an adequate OEO staff who are tasked with implementation of the OEP.

- a. Ensures USMS compliance with the OEP as stated herein, and other departmental safety orders;
  - b. Performs the DO duties at USMS Headquarters building(s); and
  - c. Ensures that an OEO is established at USMS Headquarters building(s). The OEO is tasked with the responsibility for developing, maintaining, and implementing an OEP at USMS Headquarters building(s). OEO members and their duties are contained in the DOJ Building Occupational Emergency Plan dated June 30, 1990.
2. **DO:** The DO, as the highest ranking USMS component official in a building and/or facility, shall ensure that an OEP is developed for the building or facility and that an OEO is staffed and trained to protect property and to ensure the safety of component employees in the event that the building or facility must be evacuated. The DO also ensures the OEP is updated annually.
  3. **General Services Administration (GSA):** GSA is responsible for the installation and maintenance of equipment, such as alarm systems and firefighting apparatus, in support of an OEP. GSA provides training in the use of such equipment. Assigned GSA Building Managers are responsible for providing assistance, information, guidance, and advice concerning the OEP. GSA is also responsible for conducting yearly fire drills, as required by law.
  4. **Building Manager:** Building Managers in buildings where the USMS is the prime tenant assist the USMS in recruiting qualified personnel for technical services and for arranging OEP training.

#### **F. Procedures:**

1. **Implementation:** In all buildings and/or facilities occupied by a USMS component, the DO, SPM, and Security Officer conduct the following:
  - a. Formulate and implement an OEP within 30 days of relocating to another building and/or facility;
  - b. Staff and train an OEO to coordinate all emergency procedures, following the incident command structure established in the National Incident Management System (NIMS);
  - c. Provide members of OEO with visual identifiers such as colored safety hats and/or armbands;
  - d. Maintain a current list of all individuals responsible for implementing the OEP. This list includes the DO, Alternate Designated Official, and Building Manager;
  - e. In a building where a USMS component is not the prime tenant, the DO develops an OEP with the individual selected by mutual agreement of the occupying tenants of the building, or develops an OEP for the USMS component(s) as required; and

- f. In a facility where the prime tenant has failed to develop an OEP, the USM, in conjunction with the courts, will determine who will be the DO. If the USMS is not collocated with the courts, then the senior USMS employee or his/her designee will serve as the DO.

2. **Guidance for development and implementation of an OEP:**

- a. All OEPs will:
  - 1) Provide clear instruction on the roles and responsibilities for all aspects of the preparedness spectrum, from prevention and protection to response and recovery;
  - 2) Use an approach that includes procedures to handle a wide range of hazards and threats, including medical emergencies, bomb threats, suspicious packages, natural disasters, and fire. Details should include shelter in place and shelter at workstation;
  - 3) Meet the specific characteristics, needs, and criteria for each facility;
  - 4) Involve coordination with local emergency responders and consider safety codes when developing and implementing emergency planning, such as the International Fire Code and National Fire Protection Association Life Safety Code; and
  - 5) Address multi-jurisdictional issues regarding mass care, shelter, and evacuation.
- b. General guidance concerning any aspect of the OEP can be obtained from the SPM or OEM designee; the applicable GSA Building Manager; or the USMS Safety and Health Manager, Management Support Division.
- c. An OEP Quick Reference Guide may be used for general distribution to occupants and should include facility-specific actions for occupants to take in emergency situations and floor plans with evacuation routes.
- d. The SPM procures copies of the OEP and [GSA OEP Guide](#) from the DOJ Security Officer to assist USMS Headquarters and district offices in the development and implementation of their OEP. Modifications to the model OEP are based on the building's use, occupant needs, and structural design. Changes are made to meet unique circumstances.
- e. Maintain a current file of the OEP for each building occupied by component employees and forward a copy of the OEP to the following offices:
  - 1) The building manager; and
  - 2) The Federal Protective Service at the local Department of Homeland Security office.
- f. Conduct yearly fire drills with the concurrence of the DO.
  - 1) The fire drill includes evacuation of all employees to designated locations outside the building.

- 2) The local USMS office will maintain a record of all fire drills conducted under the OEP for a period of 5 years.
  - g. Leadership of each occupant department or agency should demonstrate their commitment to facility emergency preparedness and promote an atmosphere of cooperation by authorizing staff to participate in the planning group and the OEO, and through implementation of the OEP. This commitment and cooperation can be fostered by writing memoranda to staff, establishing department or agency policy, or developing a formal mission statement that defines the purpose of the OEP and indicating that it is mandatory.
3. **OEO**
  - a. The OEO follows the Incident Command Structure, as required under NIMS, and is comprised of five major functional areas: command, operations, planning, logistics, and finance/administration. When required, intelligence may be added as the sixth functional area.
  - b. The OEO is responsible for the controlled distribution and tracking of the complete version of the OEP and will maintain an up-to-date listing of the authorized recipients so that amendments can be distributed appropriately between scheduled plan updates.
4. **OPSEC Considerations:** The complete OEP for a facility is considered to contain sensitive information. The OEP should not be posted on the Internet, but can be posted on the Intranet or other secure location. Recipients of the complete OEP typically include members of the OEO, local law enforcement and emergency service agencies, and on-site security guard force as part of post orders.

**G. Definitions:**

1. **USMS Components:** Refers to all offices, buildings, divisions, and their respective field organizations.
2. **SPM:** An individual, appointed by the Director or Deputy Director, with the delegated responsibility for the management and coordination of all security programs for USMS Headquarters and components.
3. **DO:** The highest ranking USMS component official in any building or facility occupied by one or more DOJ agencies.
4. **Security Officer:** Individuals, regardless of title, with the delegated responsibility from the SPM for the implementation and administration of security programs.
5. **Occupant Emergency Plan:** A detailed safety/security document which contains the organization and emergency response procedures that are required for the evacuation of a USMS building or facility under emergency conditions, including training of personnel. OEPs describe the actions that occupants should take to ensure their safety if an emergency situation occurs. These plans reduce the threat to personnel, property, and other assets within the facility in the event of an incident inside or immediately surrounding a facility by providing facility-specific response procedures for occupants to follow.
6. **OEO:** An organization consisting of federal employees appointed by their respective federal agency components to execute the requirements of the Occupant Emergency Plan. This organization should be limited in size and the duties of each member should

be clearly defined; however, the structure is designed to be flexible and scalable so that it may be tailored to the needs of each individual facility. Existing hierarchy of the occupant departments should help determine membership. Members should be selected by position, not name, to allow for continuity.

7. **Prime Tenant:** An organization with the largest number of employees in a building or facility. Prime tenant information concerning the DOJ and USMS can be obtained by contacting the Chief, OSP, TOD.

**H. References:**

1. Code that requires an employer to have an emergency action plan is contained in [29 C.F.R. § 1910.38](#).
2. General Provisions of Facility Management are detailed in Federal Management Regulation (FMR) [Part 102-74](#).
3. Form [USM-531](#), *Mail Bomb Recognition Poster*
4. Form [USM-531A](#), *Bomb Threat Checklist (HQ)*
5. Form [USM-531B](#), *Bomb Threat Checklist*
6. Form [USM-531C](#), *Suspicious Package Checklist*
7. Form [USM-531D](#), *Suspicious Activity Report*

- I. **Cancellation:** This policy directive supersedes Policy Directive 7.4.4, *Occupant Emergency Program*.

**J. Authorization and Date of Approval:**

**By Order of:**

**Effective Date:**

                    /S/                      
Stacia A. Hylton  
Director  
U.S. Marshals Service

August 30, 2012



## United States Marshals Service POLICY DIRECTIVES

### TACTICAL OPERATIONS

#### 17.17 SIGNIFICANT INCIDENT REPORTING

- A. Proponent:** Office of Emergency Management (OEM), Tactical Operations Division (TOD).  
Telephone: 202-307-9100, Fax: 202-451-0681.
- B. Purpose:** The purpose of this policy is to ensure the United States Marshals Service (USMS) adopts an effective, consistent, and appropriate response to all significant incidents. This directive outlines the policies and procedures for reporting significant incidents to USMS Headquarters, which in turn notifies the appropriate Department of Justice (DOJ) official.
- C. Authority:** The Director's authority to supervise the USMS is contained in [28 U.S.C. § 561\(g\)](#); [28 C.F.R. § 0.111](#); and Public Law 106-544.
- D. Policy:** The USMS is required to report significant incidents to DOJ. Reporting of these events aids in determining the appropriate initial response by the USMS and DOJ. Significant incidents are defined as distinctive or of a sufficient nature to warrant immediate notification to executive and senior USMS leadership.
1. The appropriate district or division immediately reports the following significant incidents/events per divisional reporting policy:
    - a. Shooting incident involving a USMS employee or Task Force Officer (TFO) (Refer to USMS Policy Directive 2.1, [Shooting Incidents](#));
    - b. Serious injury or job-related illness or death involving USMS personnel or another federal, state, or local law enforcement officer working with USMS employees;
    - c. Assault/attempted assault of USMS protectees; judicial officials; United States Attorneys and Assistant United States Attorneys; protected witnesses; USMS employees, or other federal, state, or local law enforcement officers working with the USMS;
    - d. Death of a prisoner in USMS custody;
    - e. Sexual assaults on USMS prisoners;
    - f. Emergencies, which include, but are not limited to, terrorist acts, riots, taking of hostages, high-jacking, kidnappings, presence of explosive devices, suspicious packages/letters, and bombings or bombing attempts;
    - g. Escape of a federal prisoner (except for a walk-away);

- h. Major arrests, including “15 Most Wanted,” major cases, and those of national interest;
- i. Adverse matters involving any aspect of foreign relations;
- j. Matters or events likely to be covered by the media with DOJ, Congressional, or Presidential interest;
- k. Any serious challenge to DOJ, Congressional or Presidential authority, or national security concerns; and
- l. Information that may warrant the personal attention of the Office of the Director, the Deputy Attorney General, or the Attorney General.

**E. Responsibilities:**

- 1. **Assistant Director (AD), TOD:** Formulates policy for and oversees the USMS OEM.
- 2. **Chief, OEM:** Serves as the USMS Headquarters point of contact for USMS Communications Center and advises both the AD and the Office of the Director on all matters concerning significant incidents.
- 3. **District/Division:** Immediately notifies USMS Headquarters when a significant incident occurs.
- 4. **USMS Communications Center:** Immediately follows established Communication Center Significant Incident notification procedures (notifies appropriate division, Headquarters senior, and executive staff).
- 5. **Division:** Responsible for establishing guidelines to USMS districts regarding the content of information required when initially reporting a significant incident to the Communications Center. Provides any assistance requested by the district. Creates and maintains a division significant incident e-mail group.

**F. Procedures:**

- 1. **District/Division Reporting Procedures.**
  - a. The district or division office involved in a significant incident immediately reports the incident to the Communications Center (Comm. Center).
  - b. The immediate notification to the Comm. Center should contain information required by the division having jurisdiction of the significant incident. At a minimum, the initial report should contain the basic information regarding the incident (refer to [Example C](#)). Due to the evolving nature of significant incidents, further updates may require clarification from the reporting entity.
  - c. The Comm. Center e-mails the preliminary report to USMS personnel assigned to the USMS Significant Incident Report List and makes verbal notification to the appropriate division(s).
  - d. Once the division(s) has been notified of the incident, it is the division(s)'s responsibility to contact the reporting office and coordinate any further assistance.



- e. Within 24 hours of the incident, the reporting office completes Form USM-210, [Field Report](#), reporting the detailed information regarding the incident, and submits the form to the appropriate division.
2. **USMS Significant Incident Report List.**
- a. Headquarters divisions are responsible for creating and maintaining a division significant incident e-mail group. This provides each division with the ability to update their own e-mail groups and ensures that the correct personnel are receiving the incident.
  - b. Each division e-mail group is added to the USMS Significant Incident Report List to ensure all divisions are receiving the incident.
  - c. The Chiefs (District) and Marshals (District) e-mail groups are added to the USMS Significant Incident Report List to ensure all district senior management are receiving notification of the incident.
3. **Department of Justice (DOJ) Reporting Procedures.**
- a. The appropriate Headquarters division prepares the [Department of Justice Urgent Report](#) in memo format as referenced below:
    - 1) [Example A: Reporting Significant Incidents](#); or *Appendix A: (blank) Significant (Urgent) Report*
    - 2) [Example B: Reporting Shooting Incidents](#); or *Appendix B: (blank) Shooting (Urgent) Report*
  - b. The draft [Department of Justice Urgent Report](#) contains the following information:
    - 1) **Points of Contact:** The name of the United States Marshal (USM), or in his/her absence, the Chief Deputy United States Marshal (CDUSM) and his/her direct office, home, or cell phone number.
    - 2) **Name of the Assistant Director:** The AD of the division that is preparing the report or, senior operational employee within the division in his/her absence and his/her direct office, home, or cell phone number.
    - 3) **Classification of the Document:** Generally, the classification is *Law Enforcement Sensitive*. If the district/division believes the report needs a higher classification, notify the Office of the Director in person or over secure communication lines to coordinate the report's completion.
    - 4) **Synopsis:** A short recitation of the facts. Do not include assumptions or inferences; rather state only the facts as they are known at the time of the report (refer to USMS directive [Field Operational Reports](#)). The division that writes the report also provides updates to the Office of the Director as information develops.
4. The draft [Department of Justice Urgent Report](#) is forwarded to the Office of the Director for review and approval.

### G. Definitions:

1. **USMS Significant Incident Report List:** An e-mail group made up of Headquarters division personnel, operational GS-14/15 Chiefs, and USMs from each district.

**H. References: None**

- I. Cancellation:** This policy directive supersedes Policy Directive 2.2, *Critical Reporting Requirements, Significant Incident Reporting Requirements*.

**J. Authorization and Date of Approval:**

**By Order of:**

**Effective Date:**

/s/  
Stacia A. Hylton  
Director  
U.S. Marshals Service

5/3/2012

**EXAMPLE A: Reporting Significant Incidents** (type in Times New Roman 12)

Appendix A: (blank) Significant (Urgent) Report

**REPORTING SIGNIFICANT INCIDENTS**  
(Urgent Report)

MEMORANDUM FOR THE ATTORNEY GENERAL  
THE DEPUTY ATTORNEY GENERAL

FROM: Stacia Hylton  
Director

SUBJECT: Urgent Report

CLASSIFICATION: For Law Enforcement Use Only

POINTS OF CONTACT:

A.	(Name)	B.	(Name)
	United States Marshal		Assistant Director
	District		Division
	Phone #		Phone #

**SUMMARY OF MAIN FACTS:** *(Where the event took place, how was notification made, date of the event, who made the notification, their phone number, and a factorial summary of event.)*

**EXAMPLE:**

The Northern District of ----- notified the Prisoner Operations Division that on (month, day, year), (Name of person involved) (what happened) while in the custody of the United States Marshals Service (USMS). (Name of person involved) was being detained on a federal writ for prosecution for possession with intent to distribute methamphetamine. On (Date), (Name of Person involved) was involved in an altercation with another federal inmate at the (facility name) and (location). He was thrown into a wall and knocked unconscious. He was taken to ABC Medical Center in (location or address). He experienced swelling of the brain and subsequently died.

The death is currently being investigated by the (name of agency). The USMS has notified the immediate family, defense counsel, the U.S. Attorney's Office, and the courts.

**LIMITED OFFICIAL USE**  
(End of Example)

**REPORTING SHOOTING INCIDENT**

MEMORANDUM FOR THE ATTORNEY GENERAL  
THE DEPUTY ATTORNEY GENERAL

FROM: Stacia Hylton  
Director

SUBJECT: Urgent Report

CLASSIFICATION: For Law Enforcement Use Only

POINTS OF CONTACT:

A.	(Name)	B.	(Name)
	United States Marshal		Assistant Director
	District		Division
	Phone #		Phone #

**SUMMARY OF MAIN FACTS:** *(Where the event took place, how was notification made, date of the event, who made the notification, their phone number, and a factorial summary of event.)*

Preliminary information received from the U.S. Marshals Office, (District), indicates that on (Date), (Number) Deputy U.S. Marshals from the (District) and two (City/State) police officers, attempted to arrest fugitive John Smith at a residence in (City/State). Smith pulled a shotgun on law enforcement personnel. One DUSM fired at least one round from his USMS AR15 and a second DUSM fired at least one round from his USMS Glock 40 caliber pistol killing the fugitive. No one else was injured.

Smith was wanted on a federal warrant for violations of supervised release. He was originally convicted for murder and had a long criminal history including charges for rape, burglary and armed robbery. The probation office issued a warrant for violation of supervised release based on new local charges of larceny and forgery.

(City/State) Police Department is conducting the investigation and the USMS Office of Inspection is responding. The DOJ Office of the Inspector General and the Civil Rights Division has been notified. (Confirm this with Office of Inspection.)

**LIMITED OFFICIAL USE**  
(End of Example)

**EXAMPLE C:** (Basic incident report)

-  
Suspicious Package Example:

On November 21, 2011 at 15:20 hrs the Northern District of ----- Courthouse received a suspicious package. All employees have been evacuated from the Courthouse. FBI and local HAZMAT teams have been notified and are en-route to the scene.

No additional information is available at this time.

POC: JSI (First Name/Last Name)  
123-456-7890 (Cell)

---

Shooting Incident Example:

On November 21, 2011 at 1750 hrs the Northern District of ----- was involved in a shooting incident. USMS Personnel responded to 1742 Main Street to arrest John Doe (FID# 0000000) who was wanted for homicide. During the arrest, shots were fired by the fugitive and USMS personnel returned fire. The subject was struck and is being transported to the local hospital.

No USMS personnel were injured during the incident.

No additional information is available at this time.

POC: SDUSM (First Name/Last Name)  
123-456-7890 (Cell)



# United States Marshals Service POLICY DIRECTIVES

## TACTICAL OPERATIONS

### 17.19 NATIONAL RESPONSE FRAMEWORK AND DOMESTIC INCIDENT MANAGEMENT

- A. Proponent:** Tactical Operations Division (TOD), Office of Emergency Management (OEM), (703) 912-2034.
- B. Purpose:** This policy directive sets forth United States Marshals Service (USMS) policy and procedures relative to the [National Response Framework](#) (NRF), and the preparation for, and response to, domestic incidents and National Special Security Events (NSSE).
- C. Authority:** The Director's authority to direct and supervise all activities of the USMS is set forth in [28 U.S.C. § 561](#)(g) and [28 C.F.R. § 0.111](#). The authority of the USMS to execute orders issued under the authority of the United States is set forth in [28 U.S.C. § 566](#). The authority of the Attorney General (AG) to delegate the performance of any of his/her functions to the USMS is set forth in [28 U.S.C. § 510](#). Additional authority is derived from [Homeland Security Presidential Directive 5](#) (HSPD-5) and the NRF.
- D. Policy:**
1. [National Incident Management System](#) (NIMS): The USMS utilizes NIMS and [Incident Command System](#) (ICS) when preparing for and responding to domestic incidents and NSSE.
  2. Delegation of authority:
    - a. Except as otherwise directed by the Director, Deputy Director (DD), Associate Director for Operations (ADO), or Assistant Director (AD), TOD, the authority to lead, direct, and coordinate USMS efforts concerning the planning for, and response to:
      - 1) Major disasters (declared under 42 U.S.C. § 5122);
      - 2) National Special Security Events (NSSE);
      - 3) States of emergency affecting multiple districts or requiring resources in excess of those available in a single district;
      - 4) Incidents or events requiring activation of USMS Continuity of Operations (COOP) and/or Continuity of Government (COG) plans or activities;
      - 5) Incidents or events requiring the deployment of USMS resources pursuant to the Emergency Support Functions (ESF) of the NRF; and,
      - 6) Other missions as assigned are delegated to the Chief, OEM, TOD.

- b. When appropriate, the AD, TOD, will designate an alternate USMS official to lead, direct, and/or coordinate these incidents or events in lieu of the Chief, OEM, TOD.
- c. The Chief, OEM, TOD, or other designated official (see above), is authorized to recruit, appoint, train, and/or deploy personnel to serve as Incident Commanders, Area Commanders, Command and General Staff, or in other capacities within the NIMS/ICS framework and to activate Emergency Operations Centers (EOC) and other coordination structures as needed to carry out his/her assigned duties.

**E. Procedures:**

- 1. Refer to [National Incident Management System](#) (NIMS).

**F. Definitions:**

- 1. Incident: An occurrence or event, natural or human-caused, which requires an emergency response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, wild-land and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response (source: NIMS).

**G. Authorization and Date of Approval:**

**By Order of:**

**Effective Date:**

/S/  
John F. Clark  
Director  
U.S. Marshals Service

8/27/10



## United States Marshals Service POLICY DIRECTIVES

### TACTICAL OPERATIONS

#### 17.20 CA NINE PROGRAM

**A. Proponent** : Canine Program Manager, Office of Emergency Management (OEM), Tactical Operations Division (TOD). Telephone: 703-912-2033. Fax: 703-603-7001.

**B. Purpose** : This directive provides United States Marshals Service (USMS) policy for the establishment, training, responsibilities, and operations of all Canine Programs.

**C. Authority**: The Director's authority to direct and supervise all activities of the USMS is contained in [28 U.S.C. § 561\(g\)](#) and [28 C.F.R. § 0.111](#). The authority of the USMS to "execute all lawful writs, process and orders issued under the authority of the United States" is found in [28 U.S.C. § 566\(c\)](#). Additional authority is derived from [28 U.S.C. §§ 564, 566](#); and [FRCrP Rule 4](#).

**D. Policy**:

1. **Mission:** The USMS uses the Canine Program for the following purposes:
  - a. To search for explosive devices, firearms, and shell casings in the safest, most expedient manner possible, considering the safety of the judiciary, the court staff, the public, and law enforcement officers.
  - b. To provide dedicated long- and short-term support to USMS missions.
  - c. To assist other law enforcement agencies, upon request and when available, in searching for explosive devices, firearms, and shell casings resulting in more interactions with these agencies.
  - d. To meet with civic groups and give demonstrations to help the public understand the missions of the USMS.
2. **Deployment:** The deployment of a Canine Team must be consistent with Policy Directive 2.1, [Use of Force](#), and all applicable USMS and Department of Justice (DOJ) policies and procedures. Canine handlers must use their dogs in a manner that does not endanger the judiciary, the court family, and/or the public. The Assistant Director (AD), TOD, and the Chief, OEM, may opt to deploy canine teams to supplement USMS missions.

**E. Responsibilities:**

1. **AD, TOD:** Formulates policy for and oversees the USMS Canine Program and approves districts' requests to establish district canine programs.
2. **Chief, OEM:** Supervises, manages, and provides oversight of the Canine Program.
3. **Canine Program Manager – Chief Inspector, OEM, and or designee:** Manages and coordinates the Canine Program at the national level.



This official develops and reviews policies concerning canine programs; evaluates, reviews, and selects training and retraining programs; and maintains administrative reports, such as monthly, annual, statistical and performance reports. Serves as the USMS liaison with Explosives Detection Canine Program (EDCP) Canine Operations, and serves as the USMS canine trainer.

**4. USM or Designee:**

- a. Reviews and signs the EDCP MOA.
- b. Provides dedicated canine vehicle from the district's motor pool and canine handler from the district's position allocation.
- c. Provides district operational review and management, including budget.
- d. Reviews and approves purchase requisitions and maintains a current inventory.
- e. Prepares and reviews employee evaluations.
- f. Gives handlers time for initial certification, daily training, and annual re-certification.
- g. Reviews all reports and notifies the USM, Chief Deputy United States Marshal (CDUSM), and division manager (if other than self) about finds and other significant events involving canine teams.
- h. Approves all deployments of canine team.
- i. Conducts periodic inspections of canine team and equipment.
- j. Ensures the canine is not used for any personal or monetary gain. The canine is restricted to official use only.

**5. 1811 Criminal Investigator (Canine Handler):**

- a. Reviews and signs the EDCP MOA.
- b. Successfully completes handler training and meets all requirements for certification and re-certification.
- c. Provides proper care for assigned canine.
- d. Continues to train the canine in the methodology taught by the training course.
- e. Follows all ATF and USMS canine policies, protocols, and standard operating procedures.
- f. Properly documents all canine records.
- g. Properly maintains canine funding.
- h. Responsible for the actions of the canine team, unless relieved of that obligation by the Canine Program Manager, CDUSM, or USM.

- i. The handler must not use the canine for any personal or monetary gain. The canine is restricted to official use only.

**6. Protection of Methods and Capabilities:** All personnel involved in the USMS Canine Program are responsible for safeguarding the specific training practices, detection capabilities, and vulnerabilities of the Program. This type of information is considered U//LES and must be protected accordingly.

#### **F. Procedures:**

**1. Request:** The United States Marshal (USM) must submit a written request to the AD, TOD, for the authority to participate in the Canine Program.

**2. Program Selection:** The OEM Canine Program will be responsible for selection, establishment, training, and operations of all USMS Canine Programs.

##### **a. Explosives Detection Program:**

- 1) The USMS participates exclusively in the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), EDCP. USMS has established a partnership with EDCP. ATF provides the canines, training, national certification, in-service training, and national re-certification to USMS. The EDCP also provides training and field support from the Training Division (TD), the Explosives Technology Branch, and the Forensics Laboratory.
- 2) The Canine Program Manager provides the USMS district with additional program information and a copy of the EDCP Memorandum of Agreement (MOA) upon request.
- 3) EDCP Program Procedures:
  - a) Review and sign the EDCP MOA.
  - b) USMS districts must establish a working relationship with the local Explosives Ordinance Disposal (EOD) unit/bomb squad and explosives detection canine unit. Specific information about the capabilities and limitations of the USMS Canine Program is considered Unclassified//Law Enforcement Sensitive (U//LES) and must be protected accordingly.
  - c) Establish a location to properly store explosives training aids. The location and storage must meet all federal explosives storage guidelines.
  - d) Select a Criminal Investigator (series 1811) applicant who has completed the Three-Year Deputy Development Program and is a current USMS Fitness-In-Total (FIT) participant.
  - e) Submit nomination and ATF MOA to the Canine Program Manager.

- f) AD, TOD; Chief, OEM; and Canine Program Manager, make district and handler selections based on regional needs of the USMS.
- g) Upon selection, the Canine Program Manager, coordinates with the ATF Chief, Canine Training and Operations, to arrange an interview.

**3. Handler      Qualifications:**

- a. Interested applicants must be series 1811 Criminal Investigator, must have completed the Three-Year Deputy Development Program, and have no pending internal investigations.
- b. Applicants must meet the EDCP prospective handler requirements (see [Appendix](#)).
- c. Applicants must be current USMS FIT Program participants.
- d. Applicants must agree to allow the canine to live inside their home and, under no circumstances, allow the dog to live in exterior kennels, garages, etc.

**4. Duty      Schedule:** Canine teams must report to work during normal business hours and be available to respond to canine-related calls on a 24-hour basis. All time attending to the care and training of the canine is compensated according to the guidelines of the [Fair Labor Standards Act](#) (FLSA) and Policy Directive 3.2, [Law Enforcement Availability Pay](#).

- a. Annual and Sick Leave: For every 8 consecutive hours of leave, 2 hours are not deducted from leave if used for canine training, not to exceed 14 calendar days.
- b. Extended Leave: In the event of extended leave (leave past 14 calendar days), the canine will be taken out of service by the Canine Program Manager until the handler returns to duty. The handler can opt to return the canine to ATF kennel for the duration of the leave or continue to take care of the canine without FLSA compensation.
- c. Handlers receive 2 hours of overtime for canine training which occurs on Saturday, Sunday, and holidays.
- d. If the canine is left with a USMS backup feeder, the backup feeder receives the 2 hours of overtime.

**5. Deployment:** Approval must be obtained from the district manager (USM or designee) before deploying the canine for any reason. Handlers must report to assignments with their canines prepared to respond and must make an on-scene determination of the appropriateness of using a canine (see [Appendix](#) for specific instructions). In the event of a find, the handler must notify the Canine Program Manager, immediately and complete and submit the necessary reports in a timely manner. Canine handlers do not conduct any render-safe operations. Render-safe Operations are turned over to an appropriately trained EOD team.

6. **Documentation/Notification:** Handlers must document all canine training, work performed (e.g., security sweep, demonstration), and maintenance and health of the canine utilizing USMS canine operations forms.

- a. Records are submitted each month to district management for review and forwarded to the Canine Program Manager.
- b. Handlers must log all finds and prepare reports immediately after deployments.
- c. Handlers must immediately notify the Canine Program Manager in the event of any illness or injuries to the canine.

**7. Funding:**

- a. District: Provides new, or newer, full time, dedicated vehicle suitable for canine transport. District is responsible for all operating costs of the vehicle. Vehicle must meet EDCP program standards.
- b. Canine Program: TOD provides funds for Canine Program maintenance to include training, overtime, equipment, and yearly maintenance of the canine team.

8. **Termination from Program:** Failure to comply with ATF/USMS Canine Program requirements, policy, and standard operating procedures or mistreatment of the canine, and/or the inability to pass certifications results in termination from this program.

9. **Retirement of Animals:** When a canine is retired or taken out of service, it must be treated in accordance with the EDCP MOA and the provisions of Policy Directive 7.1, [\*Management of Personal Property\*](#).

**G. Definitions:** None.

**H. References:** None.

**I. Cancellation:** Supersedes Policy Directive 2.4, *Operational Support, Canine Program*.

**J. Authorization and Date of Approval:**

**By Order of:**

**Effective Date:**

\_\_\_\_\_/S/  
Stacia Hylton  
Director  
U.S. Marshals Service

\_\_\_\_\_  
04/26/13

## APPENDIX A

### GUIDELINES FOR CANINE HANDLERS

**A. Handler Selection:** Applicants will be selected based on the following criteria:

1. Understands that this is a lifestyle, not just another job.
2. Able to meet all of the ATF EDCP prospective handler requirements.
3. Has a tremendous positive work ethic.
4. Is self-motivated and a self-starter.
5. Does not require close supervision.
6. Understands the 5-year commitment per the ATF MOA.
7. Applicant and family members understand the responsibility of having a police dog at their residence and the possibility that the dog may bite someone.
8. Will sign a waiver releasing the USMS and all other agencies involved in training from any liability resulting from training. (This does not eliminate any worker's compensation for job-related injuries.)
9. Can successfully pass the 10-week EDCP course in Front Royal, Virginia.
10. Extensive travel required.

**B. Uniforms:** The training/daily uniform will be consistent with the USMS uniform policy.

**C. District Equipment:**

1. **Dedicated vehicle equipped with the following:**
  - a. Full police package emergency and safety equipment; and
  - b. Communications equipment.
2. **Canine Program (OEM):**
  - a. Canine insert;
  - b. Environmental alert system (Hot Dog w/ fan & pager);
  - c. Truck Vault;
  - d. Explosives Day Box; and
  - e. Other canine equipment.
3. **Veterinary Care: Canine Program (OEM)**
  - a. All veterinary expenses incurred during the working life of the canine;

- b. Annual physicals, to include blood work, vaccinations, and heartworm testing; and
- c. Heartworm medicine (i.e., Sentinel) and flea and tick repellants (i.e., Frontline).

4. **Training Equipment: Canine Program (OEM)**

- a. Purchase food and treats for the canine.
- b. Purchase and provide Explosives training aids in accordance with ATF Training requirements.
- c. Purchase Type II day box for transportation in accordance with federal, state, and local laws.
- d. Purchase training supplies such as metal paint cans, disposable gloves, various distracter materials, and training aids. These will be continuing expenses for the working life of the canine.

**D. Care of Canine:** Handlers will be responsible for the care and treatment of their dogs at all times.

- 1. Handlers will **NEVER ABUSE THEIR CANINES.**
- 2. Handlers must be committed to being with, caring for, and training their canines every day.
- 3. Canines must be kept in a clean, safe environment.
- 4. Canines will never be left unattended in a hazardous environment, such as a hot or cold vehicle.
- 5. Fresh water will be available at all times.
- 6. Canine areas will be cleaned daily.
- 7. Canines will be taken for annual veterinary checkups.
- 8. Canines will be given a daily health check.
- 9. Canines will be given monthly heartworm and flea and tick repellant.

**E. Search Procedures:** Handlers will use their training and follow all ATF/USMS policies, procedures, and standard operating procedures when conducting searches. Also, for safety reasons districts should consult with their designated EOD unit/bomb squad to establish protocols for searches in which an explosives detection canine team assists. It is highly recommended that an EOD unit/bomb technician be on hand for canine-assisted search warrants when it is believed that an explosives device is present.

## APPENDIX B

### Selection Criteria and Information for the Bureau of Alcohol, Tobacco and Firearms' Explosives and Accelerant Detection Canine Programs

**A. General Information:** The Bureau of Alcohol, Tobacco and Firearms' (ATF) Canine Operations Branch (COB) oversees the ATF's certified detection canine team program and is responsible for selecting state and local agencies to participate in its accelerant and explosives detection canine programs. Training is provided by ATF's Canine Training Branch (CTB) at the ATF Canine Training Center in Front Royal, Virginia.

1. Agencies wishing to apply for the ATF Explosives Detection Canine (EDC) or Accelerant Detection Canine (ADC) program must complete the application form and return it to the COB.
2. All departments will be interviewed before any final selections are made for the ATF EDC or ADC program. Agencies already participating in either program will be interviewed on a case-by-case-basis (new chief, handler, etc.).
3. Interviews with departments will be scheduled ONLY after the application is received by the COB, a prospective canine handler has been identified by the department, and the department has agreed to the program's terms, outlined in the MOA.
4. An ATF canine operations branch representative as well as the prospective department head and canine handler will be present at the department's interview. Any of the department representatives who might be involved with the canine team's duties (e.g., a finance representative) may also attend.

#### **B. Prospective Department**

1. The department will be responsible for selecting its prospective canine handler. The handler should be someone who:
  - a. Is in excellent physical condition and has no health restrictions;
  - b. Has a basic knowledge of fire or explosives investigation, as appropriate;
  - c. Is not involved in any type of outside employment that could be a conflict of interest with ATF's law enforcement responsibilities or canine program commitments, such as an insurance agency, private investigation agency or canine-training business;
  - d. Will qualify under and agree to the agreements of the program as listed under "Prospective Handler"; and
  - e. Will be responsible for handling the ATF certified detection canine and no other canine during the 5-year program commitment.
2. During the handler selection process, the department should consider all additional duties that might be assigned to the prospective handler, as the ATF program requires a 7-day-a-week canine training regimen. Among the daily training responsibilities are feeding (either by training or working), grooming and exercising the canine, preparing training aids, maintaining training records,

preparing operational-use reports, and conducting canine health checks. On average, the canine can be fed/trained in approximately 1 to 2 hours. It is suggested that the canine's daily food allotment be given over the course of the day.

3. The department/handler must also select an employee to serve as a backup feeder for the canine. The employee must be someone the Agency or handler can rely on to feed the canine in the handler's absence. Backup feeders may never serve as substitute handlers. Only the designated handler who attended the ATF canine training class may use the canine operationally.
4. The department must provide the handler with a climate-controlled, full-time vehicle that has air conditioning, heat, and an installed prefabricated cage to ensure safe transportation of the canine.
5. The department will purchase food for the canine and give the handler the required maintenance training equipment. Among the training supplies that must be purchased throughout the dog's working life are metal paint cans, disposable gloves, distracter materials, and training aids (explosives/ignitable liquids).
6. After initial training is completed, the department will cover all veterinary expenses incurred during the dog's working life. Annual physical exams, to include blood work, vaccinations, and heartworm testing, are required. The department will also pay for all emergency care for the canine during its working life.
7. While the handler is in the canine-detection course, the handler's salary, overtime/holiday pay, health benefits, and any injury/illness/workmen's compensation-related claims are the responsibility of the department/handler.
8. The canine team must support the ATF National Response team (NRT). The NRT is deployed mainly to assist a state or local law enforcement agency with a large fire investigation. On average, canine teams can expect to be called once or twice a year. On those occasions the department/handler will be initially responsible for covering all travel-related expenses. Upon completion of NRT travel, the canine handler will complete an ATF travel voucher for reimbursement of all meal per diem, lodging and travel expenses. ATF is not permitted to issue hardcopy checks; all reimbursements are made via direct deposit.
9. During an NRT deployment the department will be responsible for the handler's overtime pay, health insurance, workmen's compensation, and any veterinary expenses for illness or injuries while traveling to, or working at, the NRT scene.
10. If available, the canine team must respond to requests for assistance from local or regional ATF offices. All meals, lodging and travel expenses incurred will be reimbursed. Assistance to other law enforcement agencies and fire departments is encouraged, but is provided at the discretion of the participating department.
11. All ATF canine teams must be recertified annually. The recertification process usually takes one week and is cosponsored by one of the participating agencies in various locations each year. Recertification includes an odor recognition test for the canine, practical exercises for the canine team and, if possible, classroom instruction. All newly certified teams must attend the recertification for that same year so that they will be incorporated into the yearly recertification schedule. The department will cover all travel expenses, salaries, health benefits, etc., during this process.



12. When available, the canine team is expected to attend regional in-service training, during which the department will cover all travel expenses, salaries, health benefits, etc.
13. All departments must have, or have access to, a support unit so that the canine team can be used properly. For an explosives-detection canine team, an EOD unit or an established working relationship with a local/area EOD unit or bomb technician is a must. For an accelerant-detection canine, a fire investigation unit or arson task force is recommended.
14. The department must be aware that it may not use the canine for any personal or monetary gain. The canine is restricted to official use only.
15. For safety reasons, it is recommended that the participating agency consult with its designated EOD unit/bomb squad to establish protocols for searches in which an explosives-detection canine team assists. Also, it is highly recommended that an EOD unit/bomb technician be on hand for "canine team-assisted" search warrants when it is believed that an explosive device is present.
16. Departments that apply for an explosives-detection canine have two additional expenses: They must buy and maintain a source of explosives training aids and must purchase a designated storage container (e.g., explosives bunker) to ensure that the aids are stored in accordance with federal, state and local laws. The ATF Canine Training Center will instruct handlers on proper handling and storage of their explosives training aids so cross-contamination can be avoided.

**C. Prospective Handler:** Prospective handlers must meet the following requirements:

1. The handler must be committed to being with and caring for/training the dog every day.
2. The handler must be in excellent health. Because this type of work requires excessive bending and crouching, the handler should not have any back or knee problems. The job also requires adequate upper body strength because at times the canine may need to be lifted. (Full-grown Labrador Retrievers can weigh up to 100 pounds.)
3. The handler must not be employed by any type of outside organization that could be a conflict of interest with ATF's law enforcement responsibilities or canine program commitments, such as an insurance agency, private investigation agency, or canine-training business.
4. The handler must agree to comply with the requirements to keep the dog inside the home and to never allow the dog to live in exterior kennels, garages, etc.
5. The handler must inform ATF if any other animals are living in his or her residence. It is highly recommended that other dogs living in the home be neutered or spayed, as ATF canines will not be placed in a residence with an aggressive canine. Before the training class, a member of ATF's canine training staff will interview each prospective handler to ensure that each team is properly paired and that the canine will easily adjust to the handler's living environment.
6. The handler must attend the annual recertification.

7. The handler must agree to handle only one detection canine, the ATF-certified detection canine, during his or her five-year program commitment.
8. The handler will be required to keep accurate training records and agree to comply with the ATF training methodology after completing the initial course. All handlers must bring their yearly training records to each recertification for the ATF canine training staff to review. They are also required to bring the canine's current health certificate and verification of rabies vaccination.
9. The handler will be required to submit, on a quarterly basis, all operational reports to the Chief, ATF COB.
10. The handler must be aware that he or she may be called out of town at short notice to support an ATF NRT deployment. On these occasions the NRT team leader will contact the handler and request his or her assistance, letting the handler know, if possible, how long the canine team's assistance will be needed.
11. Handlers must be aware that they may not use their canine for any personal or monetary gain but for official duties only.



# United States Marshals Service POLICY DIRECTIVES

## TACTICAL OPERATIONS

### 17.21 RADIO COMMUNICATIONS

- A. Proponent:** Office of Strategic Technology (OST), Tactical Operations Division (TOD).  
Telephone: 202-307-9485, Fax: 202-307-9366.
- B. Purpose:** This order prescribes policy, responsibilities, standards and procedures for radio communications systems and spectrum management within the United States Marshals Service (USMS).
- C. Authority:**
1. **National Telecommunications and Information Administration (NTIA).** By virtue of [47 U.S.C. § 305\(a\) \[the Communications Act of 1934 as amended\]](#), [Executive Order 12046 \[3 C.F.R. § 158\]](#), and [Department of Commerce Order 10-10 \[43 FR 24348, May 9, 1978\]](#), NTIA has the authority to:
    - a. Develop and promulgate plans, policies, and programs for United States Government telecommunications, including radio communications;
    - b. Coordinate Federal telecommunications assistance to state and local governments; and
    - c. Assign frequencies to, and amend, modify and revoke radio frequency assignments for radio stations belonging to and operated by the United States Government.
  2. **Office of Management and Budget (OMB) Approvals:** OMB Circular A-11 requires agencies to identify long-range spectrum resource requirements in budget documentation, to ensure they will receive spectrum support.
  3. **Justice Management Division/Wireless Management Office (WMO):** The WMO is responsible for:
    - a. Formulating and implementing policies, standards, and procedures for Department of Justice (DOJ) radio communication systems and spectrum management.
    - b. Approving the use of all DOJ spectrum resources.
    - c. Representing DOJ on NTIA's Inter-department Radio Advisory Committee (IRAC), its Subcommittees, and related ad hoc groups.
    - d. Interpreting and/or clarifying NTIA's *Manual of Regulations and Procedures for Radio Frequency Management* for DOJ.

- e. Serving as a DOJ representative to NTIA, OMB, and other federal agencies for radio communication and spectrum management issues.
- f. Providing spectrum guidance to components with regard to foreign radio deployment and commercial services (domestic and foreign).

The WMO delegates any of these responsibilities to any DOJ component when that component has particular expertise necessary to protect DOJ interests.

#### **D. Responsibilities:**

1. **Assistant Director (AD), TOD:** The AD, TOD, is responsible for the administration and operation of the radio communications program throughout the USMS. The AD, or his / her designee, represents the USMS on the DOJ Wireless Communications Board (WCB) and on items requiring a vote to be cast by the USMS.
2.
  - a. In accordance with DOJ Order [2422.1A](#), *Radio Communication Policy, Responsibilities, Standards, and Procedures* dated August 9, 2002, the AD, TOD, USMS designates a Spectrum Coordinator (SC), in writing, to the Director, WMO, and is responsible for keeping this designation current. The SC will:
    - 1) Oversee and be responsible for the USMS spectrum usage and planning for all USMS radio communications systems.
    - 2) Identify immediate and long-range spectrum usage and planning for all USMS components' radio communication systems.
    - 3) Serve as the Point of Contact (POC) for the WMO for its spectrum management responsibilities.
    - 4) Act as the liaison between the USMS and the WMO for spectrum dependent radio communication systems.
    - 5) Submit requests for approval to utilize or amend utilization of the radio frequency spectrum to the WMO.
3. **Deputy Assistant Director (DAD), TOD:** The DAD, TOD, is the immediate supervisor of the Chief, OST.
4. **Chief, OST:** The Chief, OST, is a GS-1811 assigned to TOD and is designated as the representative of the Director for the daily administration of the OST. The Chief, OST:
  - a. Manages the daily administration of the wireless communications program for employees of the USMS and administers the budget as provided by the WMO and USMS.
  - b. Serves as the immediate supervisor of Chief, Court Security Officer (CSO) and Courthouse Radio Program; Chief Liaison, DOJ WMO; Chief, Civilian Response Corp; and, Chief, Regional Operations.

- c. Represents the USMS on the Integrated Wireless Network (IWN) National Project Team (NPT) and provides operational evaluation and assessment of emergent radio communication technology.
  - d. Works with DOJ and the Department of Homeland Security (DHS) to ensure the USMS maintains a suitable contingency radio communication program, both short and long-range, to allow for the exercise of command, control, and communication by USMS senior staff and District management following natural disasters, national emergencies, or other critical incidents.
  - e. Assists the Training Academy with the development and maintenance of training curriculums for entry level and advanced Deputy courses of instruction.
5. **Chief, CSO Radio Program:** The Chief, CSO Radio Program, Administrative Office of the United States Courts (AOUSC), is a GS-1811 assigned to TOD and is responsible for the administration of the CSO Radio Program on behalf of the AOUSC. The Chief of the CSO Radio Program:
- a. Coordinates CSO spectrum management issues with the AOUSC.
  - b. Manages the daily administration of the wireless communications program for CSOs.
  - c. Coordinates with District Communications Officers and Judicial Security Inspectors regarding the CSO Radio Program.
  - d. Serves as the primary POC for Headquarters divisions and regarding the CSO radio program, CSO radio system infrastructure, and CSO subscriber equipment.
6. **Chief Inspector, USMS Liaison to the DOJ WMO:** The USMS Liaison Officer to the DOJ WMO is a GS-1811 assigned to TOD and is responsible for representing the USMS on the NPT and advising the Chief, OST, and the AD, TOD, on matters before the DOJ Wireless Communications Board.
- a. Serves as the primary POC for OST matters in the assigned region.
7. **Chief, Civilian Response Corp:** Chief, Civilian Response Corp, is a GS-1811 assigned to TOD and is the liaison to the Civilian Response Corp, and the United States Department of State as it relates to that mission, as well as advising the Chief, OST, and the AD, TOD, on matters relating to Civilian Response Corp Missions.
8. **Chief, Regional Operations:** Chief, Regional Operations, is a GS-1811 assigned to TOD and is responsible for the daily operations in the various regions of OST. The Regional Operations Chief:
- a. Serves as the immediate supervisor of the regional OST Inspectors.
  - b. Serves as the primary POC for the Headquarters divisions, districts, and other governmental agencies requiring specialized communication support.

9. **OST Inspectors:** OST Inspectors are GS-1811 personnel assigned to TOD and designated to assist the Chief, OST, in the daily administration of the wireless communications program. OST Inspectors:
- a. Manage the daily administration of the of the wireless communications program for their assigned region.
  - b. Supervise, support, and assist Collateral Duty Communications Officers in the performance of their duties as Communications Officers.
  - c. Provide specialized communications support, including the deployment of radio communication equipment as required, for special operations, emergency operations, and critical incidents.
  - d. Serve as the liaison between the USMS, local law enforcement, and other governmental agencies for radio communication-related issues in their region.
  - e. Represent the USMS on regional interoperability working groups and other regional project teams.
10. **United States Marshal (USM):** The USM, or designee, for each district:
- a. Designates one GS-1811 or GS-082 Deputy United States Marshal (DUSM) from the district office or major sub-office as the Collateral Duty Communications Officer for the District. This designation is made using Form [USM-222, Additional Duty Designation](#), a copy of which is forwarded to the Chief, OST. Additional persons may be designated to assist the Communications Officer as the district deems necessary; however, only one person will be designated as the primary Communications Officer for a particular district and will be the central POC for communications to OST.
  - b. Ensures all communications equipment within his/her district is properly installed and fully operational and that the WCP is carried out in accordance with this directive.
  - c. Ensures the Collateral Duty Communications Officer is allowed adequate time to administer the WCP in the district. This includes responding to OST data calls, programming and encrypting radio equipment, and serving as the USMS local POC for local law enforcement, other government agencies and local communications/interoperability committees.
  - d. Ensures Headquarters operational personnel in his/her district are given full access to the radio system used by the district and full access to the District Communications Center.
  - e. Ensures District operational employees are trained and proficient in using the district's Land Mobile Radio (LMR) system.
  - f. Promptly reports excess or unused communications equipment to OST for further reallocation or disposal.

11. **Headquarters Divisions inside the Washington, D.C., Metro Area:** Division and Unit Chiefs ensure all radio equipment assigned to their personnel is properly installed and fully operational and that their personnel are trained in using these types of equipment. Headquarters divisions/units designate a Collateral Duty Communications Officer for each of their respective division or unit. This designation is made using Form [USM-222, Additional Duty Designation](#). A copy is forwarded to the Chief, OST. OST Regional Inspectors in Springfield, VA, support Headquarters Collateral Duty Communications Officers.
12. **Headquarters Units outside the Washington, D.C., Metro Area:** Headquarters personnel assigned outside of the Washington, D.C., Metro Area utilize the radio communication systems of the district(s) in which they are assigned or operating in. Communications support is provided by the Collateral Duty Communications Officer in that district; however, providing subscriber units (mobile and portable radios) remains the responsibility of the Headquarters division.
13. **Collateral Duty Communications Officers:** Collateral Duty Communications Officers, within their respective districts:
  - a. Maintain USMS LMR subscriber equipment (portable and mobile radios) and infrastructure (base stations and repeaters) fully operational on the frequencies designated for the USMS in the districts. In addition to district-specific programming, it is necessary that all USMS nationwide zones contain standardized radio channels and naming convention to ensure nationwide interoperability.
  - b. Maintaining current encryption codes in all USMS radio equipment.
  - c. Reporting infrastructure outages (i.e., USMS, Federal Bureau of Investigation (FBI), or DHS) to the appropriate servicing Electronics Technician (ET) shop and OST Inspector when discovered.
  - d. Serve as the local USMS POC for local law enforcement, other government agencies, and as the USMS representative on any communications and interoperability working groups in the district.
  - e. Ensure the necessary frequencies are programmed in USMS radio equipment for interoperability with other federal, state, and local agencies. If required by the originating agency, the Communications Officer ensures the necessary Memorandum of Understanding (MOU) have been signed authorizing the USMS to use each respective agencies frequencies for interoperability purposes. A Draft MOU is reviewed and approved by the regional OST Inspector prior to signature by the United States Marshal (USM) of that district.
  - f. Provide assistance to Headquarters personnel located in the district (i.e., Witness Security (WITSEC), Judicial Security Division (JSD), Centers for Disease Control (CDC), Technical Operations Group (TOG)). The assistance includes, but is not limited to, programming portable and mobile radios with the frequencies designated for the USMS in that district, facilitating radio installation, maintenance, and repair, providing training on the districts radio system, and loading radios with current encryption keys. Funding for the installation, maintenance, or repair of equipment for Headquarters personnel is the

responsibility of OST and/or the respective Headquarters division, as appropriate. District Communications Officers ensure the radio communications requirements of Headquarters divisions in their district are accounted for in system designs and in any data calls.

**E. Policy:**

1. USMS personnel must only operate radio communication systems that utilize radio frequencies that have been properly assigned and approved by NTIA or the Federal Communications Commission (FCC). Written authorization in the form of a Memorandum of Agreement (MOA) must exist prior to utilization of a non-USMS/DOJ radio communications system. When USMS personnel are operating on a radio communications system, proper radio protocol and procedures must be followed at all times.
2. USMS personnel must utilize radio frequency resources only for the purpose for which the radio frequency resources have been authorized and specified in the NTIA Manual, [Chapter 7, Authorized Frequency Usage](#).
3. USMS personnel are prohibited from purchasing or using radios certified by the FCC in the [Family Radio Service \(FRS\), pursuant to Part 95 Subpart B](#) of the FCC Rules and Regulations ([Title 47, CFR](#)) for either voice communications or to exchange Global Positioning System (GPS) positioning information with other USMS users. Although the NTIA manual has a provision for allowing the use of FRS by Federal entities in limited circumstances, the rule explicitly prohibits use for planned communications operations that safeguard human life or property. In addition, FRS radios lack National Institute of Standards and Technology (NIST) approved encryption to protect the transmission of sensitive information.
4. USMS district offices and Headquarters field units must maintain, at a minimum, a fully operational base station radio or, if tied into a larger infrastructure, a dispatch console, at all district offices, large sub-offices, and Headquarters field offices.
5. All USMS radio communications must be [REDACTED]. (b)(7)(E)  
Unencrypted transmissions are allowed only in cases of exigent circumstances and to ensure interoperability in a critical incident.
6. Districts must obtain approval from the OST Inspector or Chief, OST, prior to procuring any radio communication equipment.
7. Districts must obtain approval from the OST Inspector prior to changing or adding any fixed radio infrastructure, entering into any lease agreements or an MOU and/or adding telecommunications circuits in support of radio sites.
8. No USMS radios will be programmed until the radio frequency, encryption, and configuration information or code-plug has been approved in writing by an OST Inspector.
9. This policy does not apply to any cellular telephones or satellite telephones which are not specifically designated for contingency or tactical communications purposes.
10. FCC-issued call signs are no longer valid due to the issuance of radio frequency



spectrum by the NTIA and not the FCC. The use of FCC-issued call signs promulgated in past USMS policy and training manuals is hereby discontinued.

**F. Procedures:**

**1. Transmitting on USMS Radio Communications Equipment:**

- a. Transmissions must be concise and free of inappropriate language.
- b. Oral brevity codes or “10-Codes” are not required. All transmissions must be in plain language. Districts, divisions, and/or units may adopt local “10 codes” as deemed necessary to facilitate communications during certain operations or in furtherance of task force or similar operations.
- c. The International Civil Aviation Organization (ICAO) spelling alphabet, also called NATO phonetic alphabetic, must be used to ensure uniform phraseology. The table is included herein.
- d. Transmissions for routine operations must utilize call signs and follow the procedure of “Station being called, Station being called...Station Calling.”

**2. Call Signs:**

- a. (b) (7)(E)
- b. District and sub-office base stations are called “Control” and are assigned a call sign based on the geographic location of the office. (i.e., S/NY office in Manhattan is Manhattan Control).
- c. In shared systems, where USMS call signs overlap with another agency's call sign structure, the (b)(7)(E)
- d. (b) (7)(E)
- e. USMS Task Force Officers (TFOs) must utilize (b) (7)(E)

**3. Protective or Special Assignments:**

- a. Personnel assigned to protective or special assignments may use proper last names or detail names in lieu of numeric call signs. Additional distinctive call

signs and schemes may be implemented at the discretion of the Deputy in Charge (DIC).

- b. Command Post call signs are "Command Post" or "CP". For large events where the USMS has established more than one command post, additional identifiers such as a unit name or geographic location may be necessary to distinguish between separate locations. For example, SOG CP is the Special Operations Group Command Post. The protection detail would use the detail short name (i.e. Eagle) followed by the position. Examples include: Eagle CP, Eagle Lead, Eagle Follow, Eagle Limo, etc.

4. **Radio Checks:**

- a. District offices must initiate radio checks with all subordinate offices and Headquarters field offices (maintaining a radio watch) once a day. If system infrastructure does not permit the District office to reach a sub-office via radio, then radio checks must be performed with a local unit to ensure each base station is operating properly.
- b. District offices participate in scheduled radio checks for federal interoperable radio channels, emergency channels or other radio resources as scheduled.

5. **Encryption:**

- a. Encryption keys (b) (7)(E)
- b. USMS encryption keys must not be distributed outside of the USMS without written approval from Chief, OST.
- c. Encryption (b) (7)(E)
- d. (b) (7)(E)
- e. (b) (7)(E)
- f. (b) (7)(E)
- g. (b) (7)(E)

(b) (7)(E)

6. **Radio Logs:**

- a. All base station and Command Post activities must be documented on Form [USM-66](#), *Radio Log*.
- b. The individual having actual knowledge of the facts must maintain the log, making an entry upon assuming the radio watch, and signing the log when properly relieved.
- c. No log or portion thereof will be erased, obliterated, or willingly destroyed. Necessary corrections will only be made by the original author, drawing a single line through section being corrected and initialling at the end of the line(s) containing the strike-out.
- d. Minimum information to be maintained on the radio log includes:
  - 1) The operator, assuming the radio watch must log the time he/she assumed the watch and sign the final log entry when relieved;
  - 2) A synopsis of all transmissions originated from or received by the base station;
  - 3) Any emergency messages involving safety of life or property, relays of local police broadcasts and any broadcasts relating to the National Threat Warning System; and
  - 4) A log entry will be made whenever a licensed radio technician services the base station or a USMS-owned repeater. This entry must include the name of the technician(s) and the name, address, and phone number of the company they work for. A brief synopsis of what work was done should be included if available.

7. **Emergency Radio Alarms:**

- a. In districts where system infrastructure and dispatch services support the use of emergency alarms, the emergency alarm feature will be programmed on all USMS radios in that district and all personnel will be trained in its proper use, in accordance with the following policies and procedures:
  - 1) **Permissible Uses:** DUSMs may use the emergency alarm feature on their assigned mobile or portable radio only when they reasonably believe that they or another law enforcement officer is in imminent danger of death or serious physical injury and the circumstances dictate the need for an immediate and rapid response of additional law enforcement personnel.
  - 2) **Accidental Activation:** Accidental activation of the emergency alarm feature will be reported to the appropriate communications center

immediately via voice transmission on the appropriate channel. Following the report of the accidental activation, the emergency alarm should be cleared immediately by the user on their mobile or portable radio using the appropriate button press.

- 3) Alarm Clearing: Once the circumstances dictating the activation of an emergency alarm have been brought under control and the emergency situation no longer exists, the DUSM activating the alarm contacts the appropriate communications center and advises the dispatcher that the emergency situation no longer exists. The emergency alarm is then cleared immediately by the user on his/her mobile or portable radio using the appropriate button press.
- 4) Alarm Testing: The emergency alarm feature is only to be tested by an authorized communications technician and only after the appropriate communications center has been notified of the test. No other testing is permitted under any circumstances.
- 5) Reporting Requirements: Any emergency alarm activation resulting in the response of federal, state, or local law enforcement should be reported as soon as possible to the initiating DUSM's supervisor and documented as required by the radio systems standard operating procedure.

- b. The emergency button on USMS radios will only be programmed to function as an emergency button. In districts where this feature is not available, the emergency button will not be programmed for any other use, and should be left in an un-programmed state.

8. **Spectrum Management/Radio Frequency Authorization:**

- a. As stated in Section G, Paragraph 5, subsection b, the Chief Inspector, USMS Liaison to the DOJ WMO, is designated the SC for the USMS and will oversee spectrum management issues for the operational employees of the USMS. The Chief, OST, is authorized to delegate spectrum management issues concerning the CSO Radio Program to the Chief, CSO Radio Program.

- b. Outside the Continental United States (OCONUS) Operations:

The Chief, OST, will be notified [REDACTED] prior to any anticipated operations by USMS personnel OCONUS.

(b)(7)(E)

[REDACTED] For emergency trips, notify OST via most expeditious means for an expedited frequency authorization.

9. **Contingency and Deployable Communications Equipment:** OST will maintain a suitable inventory of deployable and contingency communications equipment to support special details, emergency operations, and critical incidents.

10. **Requesting Communications Support:**

- a. How to Request: Districts and Headquarters divisions who anticipate operations

in their area that require special communications support must request such support in writing to the regional OST Inspector. All requests are reviewed and approved by the Chief of the requesting district or division before being submitted to the OST Inspector.

- b. When to Request: Requests for communications support should be submitted as far in advance as possible.
- c. Exigent Circumstances: Rapidly evolving events impacting community or officer safety may preclude a DUSM or Inspector from obtaining the appropriate written approval. In such circumstances, the OST Inspector evaluates the circumstances and determines if the situation requires immediate deployment of TOD resources. In exigent circumstances where TOD resources are deployed, a proper written request as outlined above will be generated within 48 hours whenever possible.

11. **Communications Interoperability:** DHS defines communications interoperability as "...the ability of emergency responders to work seamlessly with other systems or products without any special effort. Wireless communications interoperability specifically refers to the ability of emergency response officials to share information via voice and data signals on demand, in real time, when needed, and as authorized." Interoperable communications have an important role in USMS operations, but require specific and often detailed technical coordination between the USMS and other federal, state and local partners. It is required to ensure their proper application and to minimize the risk of compromising USMS encrypted voice traffic.

- a. Interoperability Switches/Cross Patches: No USMS radio channel will be cross patched without consulting with the regional OST Inspector, [REDACTED] or similar (b)(7)(E) interoperability devices will also not be procured or deployed without approval from OST/TOD. In addition, no radio system will be patched without the permission of the system owner in the form of an MOA. In the case of a critical incident or scenario in which a formal MOA is not feasible due to operational requirements and resulting time constraints, alternative written or verbal approval may be obtained from involved system owners and further coordinated with OST personnel. Interoperability channels and patches built into DOJ IWN radio systems have already been engineered into the radio system and are exempt from this requirement when used within the scope of the IWN. Any patches of IWN interoperable talk groups outside the realm of IWN require OST/TOD approval.
- b. Interoperable Radios: Interoperable radios are radios which operate outside the [REDACTED] used by the USMS (b) (7)(E) [REDACTED] z) and provide a means for USMS personnel to communicate with state or local law enforcement officials on their radio systems. The following guidance applies:
  - 1) The use of interoperable radios by the USMS is permitted as a secondary means of communication, and interoperable radios may either be USMS-owned or borrowed from the particular agency.
  - 2) The USMS is prohibited from conducting primary operations on any radio system outside the federal bands. DOJ policy further mandates that all DOJ components operate primarily on the frequencies assigned to their agency by the NTIA.

- 3) The use of non-federally assigned radio frequencies must be documented through an MOA from a properly authorized entity such as a state or local law enforcement agency. A copy of this MOA must be provided to OST/TOD. OST/TOD will forward the MOA to the DOJ Spectrum office for entry into the Government Master File (GMF). Any use of such resources must be in compliance with all applicable rules, regulations, and limitations imposed by the other agency or FCC.

12. **Property Management:**

- a. Nothing contained herein is intended to supersede USMS Policy regarding the handling of Accountable Property as outlined in Policy Directive 7.1, [Management of Personal Property](#).
- b. Accountable Radio Equipment: As defined in Policy Directive 7.1, [Management of Personal Property](#), LMR equipment such as portables and mobiles, infrastructure equipment such as repeaters and base stations [REDACTED] (b)(7)(E) [REDACTED] are accountable property. Interoperable radios purchased by the USMS are also accountable on USMS inventory registers. Interoperable radios loaned to the USMS by other state or local agencies are not considered accountable property, but should be accounted for locally in similar fashion to USMS property due to the obligation of the USMS to replace any lost or stolen radios.
- c. Non-Accountable Property: Accessories to radio systems such as antennas, batteries, belt clips, microphones, etc., are not considered accountable property and do not need to be entered into the USMS property management system.
- d. Inventory Requirements: A physical inventory of all accountable radio equipment will be conducted:
  - 1) During the relief process of outgoing and incoming Collateral Duty Communications Officers;
  - 2) Annually, unless a physical inventory has been conducted within 6 months for other purposes; and
  - 3) Base Station and Repeater equipment will be inspected annually.
- e. Stolen or Missing Radio Equipment: Stolen or missing radio equipment must be reported immediately to OST. Some modern radio systems provide the capability to remotely disable a stolen or missing radio. Prompt reporting enables OST to potentially disable or locate the radio and in some cases, remotely erase the encryption keys in the radio, thus minimizing damage to USMS communications security.
- f. Disposal of Excess Property:
  - 1) The Chief, OST, or designee, reviews all Standard Forms, [SF-120, Report of Excess Personal Property](#), received by Property Management that list communications equipment to ensure that equipment is not needed by another USMS entity.

- 2) If a district has located a state or local public safety agency that is in need of communications equipment that is (1) no longer used by the USMS and (2) not needed to facilitate consolidation onto FBI legacy radio systems, they should indicate on the Standard Form, [SF-122](#), *Transfer Order Excess Personal Property*.
- 3) USMS Encryption Keys and Codeplugs must be erased from any communications equipment designated as excess or otherwise disposed of.

g. Forms Use:

- 1) Initial receipt of new equipment: Form [USM-215](#), *Inventory Adjustment Voucher*
- 2) Transfer equipment between USMS offices: Form [USM-170](#), *Property Transaction Document*
- 3) Assignment of equipment within a District: Form [USM-325](#), *Hand Receipt*
- 4) Declaration of Excess Property: Form [SF-120](#), *Report of Excess Personal Property*
- 5) Transfer equipment to another Federal Agency: Form [SF-122](#), *Transfer Order / Excess Personal Property*

**G. Definitions:**

1. **Radio Communication Systems:** Any telecommunications system that utilizes radio waves to transmit voice or data. Examples of radio communication technologies include, but are not limited to: LMR, microwave data links, radar, wireless sensors, body wires, wireless video surveillance and wireless investigative search, and analysis equipment.
2. **Radio Frequency Assignment (RFA):** Authorization given by NTIA for a radio station to use a radio frequency or radio frequency channel under specified conditions.

**H. References:**

1. [Oral Brevity Codes](#)

**I. Cancellation Clause:** Supersedes Policy Directive 15.1, *Wireless Communications*.

**J. Authorization and Date of Approval:**

**By Order of:**

**Effective Date:**

          /S/            
Stacia A. Hylton  
Director  
U.S. Marshals Service

9/30/11

## **Oral Brevity Codes**

### **Phonetic Alphabet**

A	Alpha
B	Bravo
C	Charlie
D	Delta
E	Echo
F	Foxtrot
G	Golf
H	Hotel
I	India
J	Juliet
K	Kilo
L	Lima
M	Mike
N	November
O	Oscar
P	Papa
Q	Quebec
R	Romeo
S	Sierra
T	Tango
U	Uniform
V	Victor
W	Whiskey
X	X-ray
Y	Yankee
Z	Zulu





# United States Marshals Service **POLICY DIRECTIVES**

## **TACTICAL OPERATIONS**

### **17.22 MOBILE COMMAND CENTER**

- A. Proponent:** Office of Emergency Management (OEM), Tactical Operations Division (TOD).  
Phone: 703-912-2034. Fax: 703-912-2009.
- B. Purpose:** This directive establishes the policy and procedures to be followed by United States Marshals Service (USMS) personnel when utilizing the Mobile Command Center (MCC).
- C. Authority:** The Director's authority to direct and supervise all activities of the USMS is set forth in [28 U.S.C. § 561\(g\)](#) and [28 C.F.R. § 0.111](#).
- D. Policy:**
- 1. Conditions for Use:** The MCC is designed to provide an offsite command and control facility, mobile office environment, and communications platform when USMS space is not available or impractical due to geographic location, natural or manmade catastrophe, significant incident, or other event. The MCC will be deployed to support USMS personnel or approved non-USMS personnel in meeting the mission requirements of the USMS under the following conditions:
    - a. When requested by a USMS district/division in the execution of a core mission of the USMS.
    - b. When supporting a Federal Emergency Management Agency Emergency Support Function mission.
    - c. When supporting an approved state or local incident or event.
    - d. When used to promote the USMS mission to the public.
  - 2. Prohibitions:** The MCC will not be used:
    - a. As a home-to-work vehicle;
    - b. To house or transport prisoners; or
    - c. In opposition to USMS Policy Directive 7.2, [Vehicle Records and Care](#).
- E. Responsibilities:** TOD and OEM management will:
1. Ensure the MCC program is being properly managed for fiscal and operational responsibility.
  2. Provide a thorough review of each Form [USM-616](#), *Mobile Command Center (MCC) Request Form*, to ensure proper support is provided.
  3. Ensure a trained staff remains available to deploy the MCC during activations.

4. Confirm MCC Operators adhere to Policy Directive 1.2, *Code of Professional Responsibility*, and represent the USMS in a positive manner.
5. Ensure at least one MCC will be deployable at all times.

**F. Procedures:**

1. Application Guidelines:
  - a. A Form [USM-616](#), *Mobile Command Center (MCC) Request Form*, must be completed prior to a deployment unless deployed under emergency conditions. A [USM-616](#) should be completed as soon as reasonable.
  - b. Proper cost analysis should be conducted to ensure fiscal responsibility.
  - c. The requesting district/division must work with OEM to ensure proper deployment of the MCC.
  - d. Two OEM-approved operators will be deployed with the MCC. Operators will not drive over 10 hours since last 8-hour rest period (unless approved by OEM management).
  - e. The site for the MCC should be deemed safe and secure by USMS personnel for intended operations. Additional security, if needed, will be provided by the requesting entity.
  - f. The MCC should be stored indoors on USMS property, but may be stored outdoors with adequate security measures approved by OEM.
  - g. Safety of the public and USMS personnel will be paramount in all MCC operations.
  - h. Any damage caused to/by the MCC will be immediately reported to OEM management and documented in accordance with Policy Directive 7.2, [Vehicle Records and Care](#).
  - i. OEM approval is required for any MCC modifications/repairs.
  - j. The MCC will only be used for the approved mission. OEM approval is required for any mission modification.
2. Collateral Duty MCC Operator: Collateral Duty MCC Operators will be selected on a volunteer basis under the following criteria:
  - a. Operators must be USMS operational employees of the GS-1811 series.
  - b. Operators cannot be under investigation by the Office of Inspection. If an operator becomes the subject of such investigation, he/she must inform OEM management.
  - c. Operators must be approved by both OEM and their respective district/division management.
  - d. Operators must sign an MCC Operator Standards of Conduct form and successfully complete all required training.

3. Collateral Duty MCC Operator Training: The following training protocols will be followed:
- a. As selected by OEM management in conjunction with district/division management, USMS operational personnel will be trained and monitored for efficiency on the proper use and operation of the MCC.
  - b. A training program will be designed and approved by OEM personnel to cover training topics deemed appropriate.
  - c. Training will include procedures for driving, setup, and operation of the MCC.
  - d. MCC Operators may be required to complete additional training, such as Incident Command System (ICS) training, as deemed appropriate by OEM management.
  - e. MCC Operators must complete annual recertification training conducted/approved by OEM.
  - f. All MCC operators' training files will be retained by OEM. According to [General Records Schedule 1](#), Item 29, OEM will destroy these files when they are 5 years old.
4. Safety:
- a. Operation of an MCC should always be conducted in a manner posing the least risk of health or life to operators, employees, and the public.
  - b. MCCs should be inspected to the manufacturer's recommendations to ensure safe operation.
  - c. In any instance where an MCC must pull over on the shoulder of a roadway, cones will be deployed around the vehicle and operators will wear reflective safety vests, which are issued to every MCC Operator. Two additional vests will be maintained in each MCC.
  - d. Operators should never operate an MCC above their training or capabilities.
  - e. MCCs should only be used in the manner in which they were intended.
  - f. MCC operations will comply with USMS Policy Directive 7.2, [Vehicle Records and Care](#), and all other applicable policies.

**G. Definitions:** None.

**H. References:** [OEM Intranet site](#).

**I. Cancellation:** This is a new policy directive and remains in effect until superseded or cancelled.

**J. Authorization:**

By Order Of:

Effective Date:

          /S/            
Stacia A. Hylton  
Director  
U.S. Marshals Service

          05/21/2013