Department of the Interior
Law Enforcement Policy

Effective Date: March 9, 2016
Series: Law Enforcement and Security
Chapter 16: Law Enforcement Radio and Telecommunications Systems

Originating Office: Office of Law Enforcement and Security

16.1 Purpose. This chapter establishes guidelines for implementing policy and standards for law enforcement radio and telecommunications systems.

16.2 Scope. This policy applies to all law enforcement officers (LEOs) of the Department of the Interior (Department/DOI).

16.3 Authority. This policy is issued pursuant to 112 DM 17 and 212 DM 17.

16.4 Responsibility.

A. Director, Office of Law Enforcement and Security (OLES) is responsible for policy development, program guidance and oversight of the Department's law enforcement programs.

B. Bureau Directors of Law Enforcement (BDLE) are responsible for promulgating and complying with any counterpart policies or procedures as required by this chapter.

C. Office of the Chief Information Officer (OCIO) is responsible for Information Telecommunications Policy, Standards and Information Technology Security Management.

D. National Radio and Spectrum Management Office is responsible for the coordination, compliance, technical services, architecture and integration of Department radio systems and equipment.

16.6 Policy. Reliable radio and telecommunications systems for efficient communications will be maintained in all bureaus/offices with law enforcement and security responsibilities. Bureaus and offices must ensure that:

A. All law enforcement telecommunications equipment will meet Department standards and will be properly acquired and tracked with FBMS inventory controls.

B. To maintain a safe working environment, all law enforcement officers will be equipped with two-way radio equipment supported by radio systems to provide reliable access to dispatchers and other law enforcement officers.

C. Bureaus and offices will maximize officer safety by using telecommunications technology to keep track of LEOs, especially those assigned to remote locations.

16.7 Standards. Bureau/office law enforcement programs will establish and implement procedures that comply with this chapter and meet requirements specified in the corresponding *Law Enforcement Handbook*.

Law Enforcement Handbook

Chapter 16 – Law Enforcement Radio and Telecommunications Systems
Date issued: March 9, 2016

Table of Contents:

16.1 What does this chapter do? This chapter identifies standards for radio and telecommunications systems for bureaus and offices with law enforcement responsibilities.

16.2 What are the minimum bureau/office standards for radio communications? All bureaus/offices must create and maintain radio management plans/policies for the safety of law enforcement officers (LEOs) and ensure that mandatory standards detailed in this Handbook are followed, and that:

(a) All law enforcement telecommunications equipment meets Department (DOI) standards;

(b) There is property management oversight and physical security control of all telecommunications equipment;

(c) All telecommunications equipment containing law enforcement radio frequencies, or that supports encryption capabilities, including key loaders must be classified as high-risk/sensitive system- controlled property;

(d) Bureaus/offices are responsible for maintaining a current inventory in FBMS and physically accounting for all law enforcement telecommunications equipment issued or cached. Inventory records should be readily available for review upon request;

(e) Bureaus/offices will establish policies and procedures for the acquisition, storage, issuance, tracking and disposal of law enforcement telecommunications equipment in accordance with this policy and Interior Property Management Directives (IPMD 114-60).

16.3 What capabilities must each radio and telecommunications system have?

(a) Bureaus/offices must ensure that LEOs engaged in public safety law enforcement duties will have access to a two-way radio system capable of providing reliable communications with Public Safety Dispatch Center (PSDC) dispatchers, work unit LEOs, and interagency LEOs in adjoining or concurrent geographical areas. Bureaus/offices should supplement two-way radio systems with other communications systems (e.g., cell phones or satellite communication devices) when two-way radio coverage is deficient. Bureaus/offices must ensure that the all LEOs have communications systems that can access the following computer-based systems:

(1) National Crime Information Center (NCIC)
(2) National Law Enforcement Telecommunication System (NLETS)
(3) Any other computerized law enforcement information system deemed appropriate by bureaus/offices to meet operational needs.

(b) Radio systems must meet interagency communications requirements.

16.4 What general requirements must all systems meet? All radio and telecommunications systems must:

(a) Prioritize law enforcement communications transmissions to enhance the safety of DOI LEOs in performing their duties;

(b) Meet DOI telecommunications common air interface (CAI) and information security standards;

(c) Be properly managed and physically secured.

16.5 What are the requirements for accountability and tracking of LEOs?

Bureaus/offices must establish standards and protocols to utilize telecommunications systems for the accountability and tracking of LEOs including well-defined check-in procedures and requirements for regular status checks of LEOs. Managers should leverage technology such as satellite tracking devices to maximize the safety of lone workers and those assigned to hazardous work environments or tasks.

16.6 What equipment must be provided to LEOs? LEOs must be provided appropriate equipment such as portable, mobile, and base-station radios that are supported by radio system infrastructure such as repeaters, wireless microwave networks and other communications or electronic systems to enable extended geographic communication. The equipment must meet DOI operational requirements and technical standards.

(a) Bureaus/offices should identify areas where topographic challenges prevent reliable two-way radio communications and provide secondary communications systems (e.g., cell phones or satellite communication devices) to supplement or enhance communications and LEO safety. Work units that do not have 24-hour dispatch operations must establish 24-hour dispatch capabilities with other DOI bureaus or partner agencies.

16.7 May law enforcement officers use their own communication devices? Use of non-government owned communication devices is strictly prohibited for government business. This includes two way radios, satellite-based communication devices, smart phones, etc. BDLEs may approve waivers for individual use of personally-owned devices provided that LEOs and devices meet the following requirements:

(a) DOI's Office of the Chief Information Officer must provide written approval certifying that personally-owned devices have appropriate security hardware/software installed.

(b) Bureaus/offices must establish written security procedures including a signed statement from each LEO user certifying security protocol awareness and agreeing to not use personally-owned devices for government communications outside of secure communications apps or portals.

(c) Government business use of bureau-approved personally-owned devices shall not include use of personal e-mail, SMS "texting", or using devices for photography or audio/video recording under any circumstances.

16.8 What are the requirements for satellite-based communications devices? Satellite telephones, satellite two-way radios or satellite-based tracking devices must use a network that provides complete coverage of the geographic service area to include deep canyons and unique terrain. All satellite tracking and communication devices must have voice or two-way text communications capabilities.

16.9 What training must system users have? All radio users must be trained on the operational capabilities of the radio issued to them and how the system/network is designed to operate within their respective operational area including operational security, use of encryption, user controls, battery management, responsibility for maintaining physical security of issued radio equipment and immediate reporting of lost/stolen radios, etc.

16.10 Is encryption required?

(a) To provide for operational security and officer safety, all law enforcement radio communications with the exception of cellular phones and satellite phones must be encrypted. It is also recommended that devices transmitting GPS employee-tracking/location data be encrypted. Wireless devices and in-car mobile data terminals (MDTs) used to connect to the NCIC and similar law enforcement telecommunications networks must be encrypted.

(b) Bureau/office policies, procedures, and national oversight must coordinate all aspects of encryption-key management. This includes:

(1) Periodic and emergency re-keying of encryption keys;
(2) Prompt reporting, including remote disabling if possible, of lost or stolen radios and key loaders with programmed/stored encryption keys.

16.11 What language standards apply to use of radio communications? The standard for all DOI radio communications is plain language and common terminology. Unless required to communicate with interagency partners, LEOs communicating by radio should not use 10-codes or similar codes, however, they may use bureau-specific codes when appropriate to prevent suspects or others from overhearing sensitive information. LEOs must use only plain language for multi-agency, multi-jurisdiction, or multi-discipline events such as disasters, joint exercises, or special events.

16.12 How is radio spectrum assigned? Radio spectrum (frequencies) must be assigned, licensed, and used in conjunction with DOI and National Telecommunications Information Administration requirements, policies, rules and regulations. Specific guidance can be obtained in the DOI Radio Handbook (377 DM 2) and the Manual of Regulations and Procedures for Federal Radio Frequency Management (Redbook), May 2014 or newer version. The Redbook can be accessed at: http://www.ntia.doc.gov/page/2011/manual-regulations-and-procedures-federal-radio-frequency-management-redbook

(a) Bureaus/offices must assure that radio users not use radio frequencies unless the frequencies are assigned, licensed and authorized for the specific work unit and geographic location.

(b) Except for short-term emergency use, radio frequencies may not be shared between partner agencies without written DOI authorization.

16.13 How must radio programming be managed? Radio programming must be controlled and standardized within geographic areas to:

(a) Ensure that frequencies, zones, talk groups, operational controls, etc. are authorized and similar between users;

(b) Facilitate radio maintenance and ease of use;

(c) Ensure that users have access only to authorized radio networks.

16.14 What security clearances are required for users? Bureau/office personnel must have and maintain appropriate background investigations or security clearances as defined by DOI and bureau/office policy if they:

(a) Use DOI bureau/office or partner agency communications systems for law enforcement operations;

(b) Provide encryption key support; or,

(c) Provide service or maintenance of law enforcement radio systems and equipment.

16.15 What are the requirements for public safety dispatch centers (PSDCs)?

(a) All LEOs engaged in public safety law enforcement duties will have reliable access to an adequately staffed PSDC.

(b) Bureaus/offices must provide LEOs with access to 24-hour dispatch support services by DOI bureaus or partner agencies.

(c) PSDC dispatchers must be trained professionals and certified as required by bureau policy.

(d) Bureau/office units engaged in public safety and security should ensure that commonly published or posted emergency telephone numbers are promptly answered on a 24-hour basis to provide emergency assistance, or if not personally answered, that callers are provided with easy to navigate phone tree access to emergency assistance.

(e) PSDCs must be able to communicate with callers in the languages predominately spoken in each PSDC's geographic service area.

(f) Memorandums of Understanding (MOU) with originating 9-1-1 answering points/PSDCs should be established to define procedures for transferring incoming 9-1-1 emergency calls to the appropriate bureau/office PSDC or providing direct radio dispatching of bureau/office emergency responders. MOUs should include procedures for best possible response to automated requests for emergency assistance such as those generated by in-vehicle GPS navigation systems or personal locator beacons.

(g) To enable interagency coordination and plan for future transition to Next Generation 9-1-1 (NG911) or other public safety service upgrades, bureaus/offices must maintain a current national roster of all bureau-operated 9-1-1 answering points and PSDCs.

16.16 Do we have to record radio and phone communications? Automated recording equipment must be in place in PSDCs to provide for continuous recording and instantaneous playback of all public safety radio transmissions as well as all incoming public safety telephone calls. Federal requirements mandate a 180 day minimum retention period for recordings and bureau/office policies must stipulate procedures for secure storage and retention of recordings.

16.17 What safeguards apply to using and storing radio equipment?

(a) Users must safeguard equipment to prevent loss or theft and unauthorized use or monitoring of law enforcement sensitive and personally identifiable information.

(b) Users must be mindful of surroundings and audio volume. When possible, LEOs should take reasonable precautions to avoid inadvertent disclosure of confidential, law enforcement-sensitive, or personally identifiable information to members of the public, including persons being detained, interviewed or being provided with emergency medical services.

(c) Lost, stolen, missing or destroyed high-risk/sensitive system-controlled telecommunications equipment must be entered into IMARS and the DOI Internal Affairs tracking system within 24 hours of known loss. Under bureau/office policy, the circumstances of the loss will determine whether the bureau/office Internal Affairs unit must conduct an investigation.

16.18 Definitions.

(a) *Encryption device*: Electronic cipher coding hardware and software meeting Federal and DOI standards that are installed and/or programmed within radio equipment or other devices to prevent unauthorized parties from intercepting law enforcement radio transmissions.

(b) *Encryption key*: A unique electronic code key assigned to radios within a law enforcement group or work unit to encrypt and decrypt radio transmissions. Using a portable electronic key loader or over-the-air rekeying system, encryption keys must be installed within each radio to support these encryption capabilities. Encryption keys are changed frequently to maintain and enhance communication and operational security or for special law enforcement operations, or when believed to be compromised, or a potential risk exists such as when a radio is lost.

(c) *Encryption keyloader*: An electronic device meeting Federal and DOI standards that generates, stores and/or transfers encryption keys to and from a radio or another keyloader that has encryption key management capabilities and information.

(d) *Public Safety Dispatch Center (PSDC)*: A professionally operated, adequately staffed and equipped communications center with trained public safety dispatchers (and certified, if applicable) to support LEOs and other public safety professionals using telecommunications and information technology systems and networks. Support provided will include emergency assistance; tracking of personnel and equipment where feasible; coordination of responses by law enforcement, medical and fire resources to incidents; and interagency communications. PSDC dispatchers must maintain a minimum background investigation and security clearance as defined by bureau/office policy.

(e) *Radio system*: A radio system meeting DOI standards, designed with Association of Public Safety Communications Officials (APCO) Project 25-compliant (P25) technology to provide sufficient radio communication coverage to support law enforcement and public safety operations.