Attachment M

Sensitive Wireless Tactical Systems

DEPARTMENT OF HOMELAND SECURITY

DHS Policy Directive 4300A, "Information Technology Systems Security Program, Sensitive Systems"

Version 1.0

April 28, 2022

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	April 28, 2022	Initial draft updated processes and authorities Craig Basham, MSO Division Chief, IT OPS

CONTENTS

Introduction

This document provides requirements and guidance to assist Department of Homeland Security (DHS) Components in the development and implementation of their cybersecurity programs for their wireless tactical systems. It is a supplement to the DHS Management Directive (MD) 140-01-001, "*Information Technology System Security Program, Sensitive Systems*" (hereafter known as DHS 4300A) and is intended to be read in conjunction with that document, especially Section 4.0. Within Instructions M, the use of the word "shall" shall be considered mandatory only in as it applies to existing DHS policy elements. Instructions M also includes concepts and practices from other federal entities with established wireless security programs, such as the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), and the Department of Defense (DoD).

1.1 Purpose

The purpose of this document is to further define DHS wireless security policy beyond DHS 4300A as it pertains to wireless tactical systems in a sensitive but unclassified (SBU) environment. It provides a minimum set of management, operational, and technical controls that DHS Components are required to implement and with which they are expected to monitor compliance. It also suggests best practices and options that DHS Components should consider when managing their wireless tactical systems.

1.2 Scope

This document addresses the cybersecurity of wireless tactical systems. While wireless tactical systems could involve a variety of different technologies, this document specifically targets land mobile radio (LMR), Marine Band very high frequency (VHF) frequency modulation (FM), ultra-high frequency (UHF) subscriber devices and infrastructure equipment, mobile applications for tactical voice communications, and high frequency (HF) voice and data systems in an SBU environment.

1.3 Authority

This document is issued as user guidance under the authority of the Chief Information Officer (CIO) through the Office of the Chief Information Security Officer (CISO). It supersedes directives of the departments to which the Components formerly reported. For topics not covered in the DHS 4300A compilation (which includes this document as well as other supplements), departmental directives shall remain in effect until relevant DHS policy and implementing guidance are issued.

1.4 Wireless Tactical Systems

Wireless tactical systems include LMR VHF and UHF subscriber devices and infrastructure equipment, Marine VHF FM radio subscribers, HF voice and data devices and infrastructure equipment, remote sensors, mobile applications for tactical voice communications, technical investigative and communications systems, protective communications systems, mobile applications for tactical voice communications and their specific configurations. Because they are often deployed under circumstances in which officer safety and mission success are at stake, wireless tactical systems require even greater cybersecurity measures than those employed with

other wireless communications technologies. To ensure encrypted tactical communications, Components must implement strong identification, authentication, and encryption protocols designed specifically for each wireless tactical system and their specific hardening and setting configurations. The following table is found in the DHS 4300A.

DHS Policy
a. Authorizing Officials (AOs) shall be immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents.
b. Wireless tactical systems shall implement strong identification, authentication, and encryption for their various configurations. Configuration hardening, setting and operating procedures should be considered.
c. Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless tactical system being approved for use.
d. Components shall maintain a current inventory of all approved wireless tactical systems in operation.
e. Legacy tactical wireless systems that are not compliant with DHS Information Technology (IT) security policy shall implement a migration plan to outline the provisions, procedures, and restrictions for transitioning these systems to DHS-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception from the CISO, as appropriate.
f. The security configuration of LMR subscriber units shall be validated via over-the-air-rekeying (OTAR) or hard rekey using a crypto-period no longer than 180 days.
g. All LMR systems shall comply with Project 25 (P25, EIA/TIA-102) security standards where applicable.

1.5 Structure of the Policy Directive

The remainder of this document is divided into the following sections:

- Section 2 (Governance) discusses the management controls and structure supporting wireless tactical systems security.
- Section 3 (Standard Operating Procedures) describes how Components should document their operational practices to support wireless tactical systems security, with a focus on LMR operations.
- Section 4 (Technology) focuses on the features that must be considered when acquiring and configuring LMR systems and networks, although some concepts may apply to wireless tactical systems more generally.
- Section 5 (Training and Exercises) reviews methods for ensuring staff are aware of security threats and requirements and can use their wireless tactical systems in an encrypted mode.
- Section 6 (Usage) explains how the controls and practices listed in the previous section might be implemented over time.

Each of the sections listed above corresponds to an element of the *SAFECOM Interoperability Continuum and the DHS Interoperable Communications Act Strategic Plan*, which are designed to help the public safety community and federal policy makers address critical elements of success as they plan and implement interoperability solutions. Many organizations are reluctant to implement cybersecurity mechanisms because of a concern that they could impede

interoperability. Integrating cybersecurity requirements into an interoperability framework helps alleviate this concern because it demonstrates the potential synergy between cybersecurity and interoperability.

1.6 Revisions to the Policy Directive

The Wireless Management Office (WMO) publishes this policy directive and is responsible for any revisions to it. All proposed revisions are presented to the DHS Wireless Security Board (WSB) for review and comment. WSB members can also introduce proposed revisions to the document during WSB proceedings.

Any feedback on or suggested revisions to this handbook should be forwarded to relevant Component's representative to the WSB. The WMO can be contacted to obtain information concerning WSB membership.

Future revisions of this document are expected to include additional material on non-LMR wireless systems used in tactical environments.

2.0 GOVERNANCE

Governance assures that appropriate security controls are selected, that the necessary resources are allocated to implement these controls, that performance is monitored, and that corrective actions are taken when shortcomings are identified. Governance will happen at multiple levels across the Department/Components and within the Components themselves for execution.

2.1 Wireless Management Office

The WMO, a component of the office of the CIO, formulates and coordinates department-wide policies and guidelines related to the security of wireless services and technologies, including wireless tactical systems. The WMO established the WSB to assist it with this mission. The WSB is co-chaired by the Department's information technology (IT) security organization to ensure consistency in the development and implementation of risk management approaches and certification and accreditation (C&A) processes for wireless services and technologies. The WSB also assists DHS in the development, deployment, and maintenance of wireless security strategies for major wireless IT programs and system development initiatives. In addition, the WSB serves as a forum for identifying and resolving emerging wireless security issues and concerns.

This document represents the WMO's primary mechanism for providing policy and guidance with respect to wireless tactical systems.

2.2 Future Developments

Governance related to wireless systems, including wireless tactical systems, will evolve over time. Some future developments will likely include the following:

- Additional guidance related to the certification requirements for wireless tactical systems that addresses specific technologies and protection mechanisms.
- Development of guidance for tactical communication applications that mimic LMRs through mobile platforms.

- Additional guidance relating to Next Generation (NextGen) technology devices.
- Sharing of governance best practices across DHS so that Components can improve their internal governance of wireless tactical systems.
- Development of governance structures involving organizations outside of DHS in order to support interoperability of communication across DHS Components and state, regional, tribal, territorial and other federal government entities.

3.0 STANDARD OPERATING PROCEDURES

Operations security (OPSEC) is a critical component of cybersecurity. Standard operating procedures (SOP) provide a foundation for OPSEC because they enable consistent practices, make designated personnel accountable for the performance of those practices, and provide a baseline against which auditors can measure that performance.

3.0.a. Each Component SHALL maintain SOPs for each of the following areas:

- Key Management
- Configuration Management
- Security Incident Response
- Temporary Suspension of Security Controls
- Continuity of Operations Plan (COOP)
- Radio over Internet Protocol (RoIP) Network Patching

3.0.b. Each Component MAY maintain separate SOPs for different organizational elements (e.g., divisions, branches, or, in some cases, job categories), if every organizational element is covered by compliant SOPs.

3.0.c. Each Component SHALL submit its SOPs to the WMO so that it can review the SOPs' security procedures and requirements for compliance with DHS 4300A.

The remainder of this section explains the content of each SOP in more detail. Components are given the discretion to write SOPs in a manner appropriate to their mission and operational environment; in most cases, the SOP requirements listed in this document address the required coverage of each SOP rather than its implementation details. In some cases; however, the guidance provides a minimum department-wide standard.

3.0.d. Components SHALL include minimum departmental standards in each applicable SOP.

3.0.e. A Component MAY exceed a minimum departmental standard, thereby providing additional cybersecurity, if it determines that a higher standard is required to fulfill its mission.

3.0.f. SOPs SHALL include the following:

- Date and version of the SOP;
- Letter of approval/review from the WMO;
- Contact information for security-related questions about the SOP; and
- Any standard DHS notices or warnings.

3.1 Key Management

Cryptographic keys are required to adequately support cybersecurity objectives, particularly those related to confidentiality, integrity, authentication, and non-repudiation. Key management refers to the generation, distribution, storage, and destruction of cryptographic key material.

3.1.1 Key Generation

Cryptographic keys are generated by computers to ensure that they meet the requirements of the algorithm that they support and that they are sufficiently random, which is, in part, what makes the cryptosystem difficult to exploit. In the case of wireless tactical systems, a key management facility (KMF) typically generates required keys.

3.1.1.a. The Key Management SOP SHALL identify either (1) the specific hardware and software authorized for key generation or (2) the external entity authorized to provide keys. All key management hardware and infrastructure SHALL be compatible and provide and process the latest specified key configurations and key length provided by NIST and NSA Standards.

3.1.1.b. When an organization generates its own keys, the Key Management SOP SHALL specify the personnel or roles authorized to operate and administer key generation technology and the responsibilities of those personnel or roles.

3.1.1.c. All personnel authorized to generate keys SHOULD be trained in the proper generation and handling of the keys, including the requirement for secrecy.

3.1.1.d. If keys from external entities are required for interoperability purposes in the communications of SBU information, then the Component SHALL receive approval from the CISO before using such keys.

3.1.1.e. If SBU keys are obtained from an external entity other than the NSA to support interoperability, then the Key Management SOP SHALL—

- Specify the persons or roles permitted to receive keys and handle key material;
- Require that the person receiving a key record the date and time the key was received and the name and affiliation of the person from which the key was received; and
- Implement a process by which someone can trace each externally supplied key in use to its source.

3.1.2 Key Distribution

Keys must be distributed to each communication device for encrypted communications to occur. If protected keys are revealed during the distribution process, the security properties of the cryptosystem are lost. To help ensure privacy is maintained, keys are either distributed out-of-band (i.e., using a different medium than the one over which subsequent communications will occur) or are encrypted prior to transmission. In wireless tactical systems, a common out-of-band mechanism is to establish a wired link from the LMR subscriber device and/or infrastructure equipment to a key variable loader (KVL). Another method to distribute keys is over-the-air rekeying (OTAR), typically using a wireless connection between the LMR subscriber device and/or infrastructure equipment and a KMF. OTAR provides centralized key management and can quickly distribute keys to many LMR subscriber devices and/or

infrastructure equipment nearly simultaneously. However, because over-the-air communication is not out-of-band, keys must be encrypted with a key encryption key (KEK), often called a shadow key.

3.1.2.a. The Key Management SOP SHALL specify the chosen authorized methods for key distribution.

3.1.2.b. The specified method SHALL either involve out-of-band distribution or encryption of keys prior to distribution.

3.1.2.c. All key distribution transactions SHALL be logged. The log records SHALL be protected against unauthorized modification and retained for a period of at least one (1) year.

3.1.3 Key Storage

Keys must be kept at their same classification level during storage as well as distribution. All LMR subscriber devices and/or infrastructure equipment participating in encrypted communication must store keys, even if, in some cases, only temporarily.

3.1.3.a. Keys SHALL be stored in an encrypted format.

3.1.3.b. The Key Management SOP SHALL specify the authorized locations in which keys are permitted to be stored.

3.1.3.c. Keys that are removable from LMR subscriber devices and infrastructure equipment, such as keys stored on tokens or hard copy versions of keys, SHALL be physically secured when not in use. The physical security SHOULD be in accordance with DHS 4300A's General Physical Access policy and DHS IT Security Architecture Guidance Volume II: Security Operations and Support.

3.1.4 Key Destruction

When keys are no longer in use, they MUST be destroyed in order to protect past communications. If an adversary had recorded encrypted radio conversations, subsequent acquisition of the key used to encrypt the communications would reveal its content, which could provide the adversary with sensitive information on the organization's tactical operations.

3.1.4.a. The Key Management SOP SHALL specify the procedure to sanitize storage media containing key material after it is no longer required for operations.

3.1.4.b. The sanitization procedure SHOULD involve technology other than simple file deletion. It MAY involve degaussing magnetic media, using disk-wiping utilities, over-the-air zeroization, or physical media destruction.

3.1.4.c. Key material stored in a hard copy format SHALL be either shredded, burned or pulped when that key is no longer required to support operations.

3.1.5 Suspected Key Compromise

An adversary can compromise a key through many different means, including acquiring the key from a lost or stolen LMR subscriber device or infrastructure equipment, using access (perhaps authorized) to a KMF for nefarious purposes, or cryptanalysis. Personnel may suspect key compromise for a variety of reasons. In some cases, loss of an LMR subscriber device or

infrastructure equipment or known unauthorized access to a KMF is enough to suspect key compromise. Key compromise also might be suspected if targets of a tactical operation take actions that imply knowledge of encrypted communication. If personnel receive unauthorized messages over an encrypted channel or talk group, then key compromise is almost certain.

3.1.5.a. The Security Incident Response SOP SHALL instruct any person suspecting a key compromise to report it immediately.

3.1.5.b. The Security Incident Response SOP SHALL specify to whom the suspected key compromise reporting should be directed. This SHOULD be a security operations center or on-call security operations personnel.

3.1.5.c. The recipient of a suspected key compromise report SHOULD notify the Component Information System Security Officer (ISSO) as soon as practicable. This notification MAY NOT be immediate if the original report was received outside of business hours.

3.1.5.d. The Security Incident Response SOP SHALL specify the options for communicating suspected key compromise. These options SHALL include both telephone and e-mail.

3.1.5.e. The Security Incident Response SOP SHALL specify a verbal code to use when performing in-band reporting of a suspected compromise. Such reporting MAY be necessary during a tactical operation if alternative means of communication are unavailable but SHOULD NOT be used if alternative means are available.

3.1.5.f. The Security Incident Response SOP SHALL specify the process for determining when a report of a suspected compromise warrants a response. The process SHOULD anticipate the need for a response within four () hours. It MAY involve an order from the ISSO, or systems operations personnel MAY be given authority to act without approval under special circumstances to be specified in the SOP.

3.1.5.g. If it is determined that a response to a suspected key compromise warrants a response, the response SHALL include rekey of any such key on all devices that possess the key.

3.1.6 Periodic Rekeying

The longer a key remains active, the more likely it is that an adversary has compromised the key using techniques such as cryptanalysis, theft, or social engineering (i.e., establishing and misusing a trusted relationship with an individual who has authorized access to key material). To reduce the likelihood of a successful attack, keys are periodically replaced. Close coordination is critical during rekeying procedures to ensure that all LMR subscriber device and/or infrastructure equipment have the same key; if any LMR subscriber device and/or infrastructure equipment continue to use retired keys; they will be unable to participate in coded communications.

3.1.6.a. The Key Management SOP SHALL specify the frequency of key replacement for Component traffic encryption keys (TEK) and SHOULD not exceed a 30-day key cycle.

Key cycles exceeding 30 days SHALL require a waiver from the DHS CISO, with WMO review and concurrence. A waiver MUST be based on mission essential requirements and

justification for extended key cycles. Waivers SHALL not authorize more than a 180-day key cycle.

3.1.6.b. Key Encryption Keys (KEKs) that are shared across multiple LMR subscriber devices and/or infrastructure equipment SHOULD be replaced periodically. KEKs that uniquely identify an LMR subscriber device and/or infrastructure equipment MAY be kept in service indefinitely.

3.2 Configuration Management

Configuration management controls changes to wireless tactical systems to ensure that these changes are consistent with the organization's mission and tactical objectives. It often enables technical support personnel to quickly identify the root cause of operational problems and allows security personnel and auditors to detect malfeasance or other violations of policy.

3.2.a. Each Component SHALL maintain documentation on the encryption configuration state of each wireless tactical system it operates.

3.2.b. Each Component SHALL establish a written change approval process for each wireless tactical system it operates.

3.2.c. The Configuration Management SOP SHALL specify the membership of the Configuration Control Board (CCB). The CCB membership SHOULD be based on personnel roles rather than named individuals.

3.2.d. The Configuration Management SOP SHALL specify the procedure by which each proposed change SHALL be brought before the CCB for approval. The procedure SHOULD include a description of the information that must accompany each change request (CR). The CR information SHALL, at a minimum, include the following:

- The purpose of the change;
- The specific equipment or systems that the change will impact;
- The date and time the change will be performed;
- The duration of the work;
- Whether the change is expected to cause a temporary outage or performance degradation;
- The personnel who will be performing the change; and
- The rollback procedure in case the change does not have its intended effect.

3.2.e. The Configuration Management SOP SHALL specify the voting procedure for CR approval. Approval SHOULD require unanimous written consent of the CCB membership. Written consent MAY be electronic, such as through an e-mail message or an authenticated entry in a configuration management software tool.

3.2.f. The Configuration Management SOP SHALL specify an emergency change procedure for any configuration changes that need to occur prior to a meeting of the CCB in order to restore the availability or security of the system.

3.2.g. The Configuration Management SOP SHALL require timely submission of an emergency CR for retroactive approval of each emergency change. The time frame for submission of an emergency CR SHOULD be no longer than 48 hours after the change. The

Configuration Management SOP SHOULD require that the system be rolled back to its state prior to the emergency whenever an emergency CR is not approved.

3.2.h. The Configuration Management SOP SHOULD include controls related to the appropriate separation of duties. Individuals who develop software, scripts, or radio programming instructions SHOULD NOT be permitted to implement the software, scripts, or instructions on operational systems.

3.2.i. The Configuration Management SOP SHALL specify the procedure by which technical personnel document the completion of an approved CR. The procedure SHOULD include a description of the information that must accompany each after-action report (AR). The AR information SHOULD include the following:

- Who performed the work specified in the CR;
- Whether the work was performed successfully;
- If the work was not performed successfully, whether the rollback procedure was performed successfully;
- Whether any steps had to be added or removed to achieve the desired result; and
- The date and time the work was started and finished.

3.2.j. Retirement or disposal of system hardware SHALL be considered a configuration change. The Configuration Management SOP SHALL specify the procedure for sanitizing media of key material and other sensitive data prior to disposal. The authorized techniques SHALL NOT include simple file deletion. They may include zeroization or degaussing.

3.2.k. The Configuration Management SOP SHALL specify the recordkeeping requirements of CCB proceedings. Approved CRs and approved ARs SHALL be maintained for a period of not less than one (1) year. They SHOULD be maintained for the operational lifetime of the system.

3.3 Security Incident Response

Most security controls are designed to protect an organization against cybersecurity threats; however, regardless of how effective those controls are, some security incidents are inevitable. Organizations need to have an effective response capability in place before the occurrence of such events.

3.3.a. The Security Incident Response SOP SHALL specify methods for communication device users and other personnel to report security incidents, in accordance with DHS 4300A, Instructions F. One of the methods SHALL be via a telephone call to security operations center or on-call security operations personnel.

3.3.b. The security incident response capability SHOULD be available on a continuous basis (i.e., 24 hours a day, 365 days a year).

3.3.c. Each security incident report SHOULD include the following:

- Equipment or technology involved (i.e., make, model, etc.);
- Event (e.g., loss, theft, no longer operational);
- Personnel involved;

- Location of incident;
- Circumstances of incident;
- Possibility of compromise; and
- Point of contact.

3.3.1 Lost or Stolen LMR Subscriber Device

If an adversary either steals an LMR subscriber device or obtains a lost LMR subscriber device, then the adversary can listen to or participate in sensitive communications. A malfunctioning or tampered-with LMR subscriber device can also compromise the security of the system.

3.3.1.a. The Security Incident Response SOP SHALL specify the procedure that SHALL be followed to report a lost, stolen, malfunctioning, or tampered-with LMR subscriber device. The procedure SHALL specify that such reporting occur immediately or as soon as it is feasible to do so.

3.3.1.b. The Security Incident Response SOP SHALL specify the actions that a systems administrator and owner SHALL take in response to notification of a lost, stolen, malfunctioning, or tampered-with LMR subscriber device. These actions SHALL include preventing the LMR subscriber device from authenticating to the LMR network or participating in a talk group. The actions SHOULD include rekeying all LMR subscriber devices holding the same TEKs as the lost, stolen, malfunctioning, or tampered-with LMR subscriber device. The actions SHOULD include over-the-air zeroization of key material if this feature is available.

3.3.2 Radio Frequency Interference

Radio interference is the presence of electromagnetic radiation on the same radio frequencies needed to transmit voice or data traffic. Radio users typically will be able to detect interference from the persistent dropping of connections, unusually slow traffic, or the existence of noise on a channel or talk group. Interference can be either unintentional or intentional. Unintentional interference might be the result of another agency using a similar wireless communications system in the same vicinity. Intentional interference, also referred to as jamming, occurs when an adversary is deliberately attempting to disrupt communications. As the need for spectrum increases and the amount of spectrum available decreasing, there are increased risks of interference.

3.3.2.a. The Security Incident Response SOP SHALL specify the actions to take after radio users detect radio interference. The actions SHALL at a minimum include:

- Notifying a relevant authority that the interference is occurring
    - The first authority should be within the Component and associated stakeholders.
    - If interference continues, contact the WMO Spectrum Management Team to assist.
- Mitigating the impact of the interference

3.3.2.b. The first technical approach to interference impact mitigation SHOULD be to change frequencies, if the radio technology supports this approach.

3.3.2.c. If radio interference is expected or is common that cannot be circumvented through changing the frequency, then tactical personnel SHOULD have the ability to switch to a backup form of wireless communications. The backup MAY be the use of a commercial cellular telephone.

3.3.2.d. The Security Incident Response SOP MAY cover procedures for the identification of the source of interference through triangulation or other means. If such procedures are included, they SHOULD include methods of evidence collection that would allow for subsequent prosecution of illegal behavior.

3.4 Temporary Suspension of Security Controls

In many tactical operations, availability of communications is considered significantly more important than the confidentiality or integrity of those communications. In these situations, tactical operations personnel sometimes override or deactivate security controls such as encryption when they are preventing communication. Such actions are infrequent if not nonexistent on well-configured systems with mature SOPs. Nonetheless, provision for such an occurrence is appropriate in scenarios in which temporarily suspending security controls likely will save lives or prevent significant property damage, especially if the risk of eavesdropping is low.

3.4.a. The Temporary Suspension of Security Controls SOP SHALL specify the roles that are authorized to permit the temporary suspension of security controls. The authorized roles SHALL NOT include LMR subscriber device users. They MAY include an incident commander, system owner, or ISSO.

3.4.b. The Temporary Suspension of Security Controls SOP SHALL specify the conditions under which override is permitted. These conditions SHALL include (1) critical communication cannot occur without override and (2) delay MAY lead to a significant adverse consequence.

3.4.c. Temporary suspension of controls SHALL NOT be invoked to support interoperability unless it is determined that there is no means to bridge communications. Bridge communications options MAY include the use of special technology designed for that purpose or selecting personnel to hold multiple LMR subscriber devices.

3.4.d. The system's Authorizing Official (AO) (Note: Authorizing Official replaces the term Designated Accrediting Authority (DAA) as per NIST SP 800-37.) and ISSO SHALL be notified as soon as practicable whenever security controls are temporarily suspended.

3.5 Continuity of Operations Planning

Continuity of operations planning (COOP) helps ensure that communications technology is available to support tactical requirements.

3.5.a. The COOP SOP SHALL specify the roles and responsibilities of personnel during a significant system outage. A personnel notification roster SHOULD be distributed among all relevant personnel for use during emergencies or significant outages.

3.5.b. The COOP SOP SHALL specify the circumstances under which personnel should operate LMR subscriber devices in ad hoc or peer-to-peer (P2P) mode (e.g., when infrastructure connectivity is unavailable).

3.5.c. The COOP SOP SHALL list other authorized mechanisms for receiving and transmitting information when tactical systems are unavailable. Such mechanisms MAY include the use of commercial cellular telephones or, for broadcast purposes, broadcast radio or Internet websites.

3.6 Radio Centric IT Infrastructure Systems and Network Patching

IT based systems require periodic updates and patching as prescribed by the manufacturer, vendor, security office or as deemed by DHS as part of configuration management. These updates and patches provide enhancements to the systems regarding operation, function and security. Components need to have an effective patching capability in place before processing of updates and patches.

3.6.a. Components SHALL develop and maintain a Configuration Management SOP, to include patching and implementing updates to system components and infrastructure. The Configuration Management SOP SHALL specify methods, processes, and requirements for these actions.

3.6.b. Components SHALL perform vulnerability scans on supported test systems using third-party scanning tools to identify and address new vulnerabilities and compliance issues.

3.6.c. Configuration management policies MUST include provisions for quickly testing and approving time-sensitive changes that result from newly released vulnerability information.

3.6.d. Patches and updates SHOULD be implemented once tested and validated.

3.6.e. Components SHALL monitor for and obtain alerts from Cybersecurity & Infrastructure Security Agency (CISA), DHS CISO, Information Assurance Vulnerability Management (IAVM) alerts issued by the DoD Computer Emergency Response Center (DoD-CERT), and Original Equipment Manufacturer (OEM) Bulletins and updates as appropriate.

3.6.f. Components SHALL install security and software patches no later than 30-days after release from the LMR/Tactical Communications OEM.

3.7 Future Developments

SOPs will undergo continuous improvement as operational practices mature and technology is upgraded. Some future developments likely will include the following:

- SOPs to support interoperability across multiple DHS Components or federal agencies, or between state, regional, tribal, and territorial entities supporting tactical operations;
- SOPs to support the creation, use, and break-down of ad hoc or P2P networks when centralized infrastructure is unavailable or for any other reason;
- SOPs/guidance on the use of tactical communication mobile applications;
- SOPs/guidance on the use of Bluetooth applications within tactical communication devices;
- Improved guidance on identifying and avoiding radio interference;

- Technology-specific guidance providing step-by-step instructions on how to implement security controls on a make and model of an LMR subscriber device and/or infrastructure equipment or its supporting equipment; and
- Guidance related to the development of system specific Rules of Behavior, in accordance with DHS DM 140-01-001, Instructions G.

4.0 TECHNOLOGY

Properly configured technology is a critical component of cybersecurity. This section covers acquisition and configuration requirements to ensure that wireless tactical systems are compliant with DHS and Federal Information Processing Standard Publication (FIPS PUB) requirements and that they support the SOPs discussed in Section 3.0.

4.1 Acquisition Requirements

The acquisition of a new wireless tactical system is a significant long-term investment. Strict acquisition guidelines ensure that Components select wireless tactical equipment that complies with DHS 4300A policies and supports the configuration requirements described in this handbook. The acquisition requirements discussed in this section include Tactical Communication II (TACCOM II) Indefinite Delivery/Indefinite Quantity (IDIQ) contract vehicle for acquisition guidelines, Project 25 (P25) compliance to ensure interoperability in an encrypted environment, and FIPS 140 topology compliance to ensure confidentiality.

4.1.1 TACCOM II IDIQ Compliance

Working with the U.S. Customs and Border Protection (CBP), the WMO and Joint Wireless Program (JWP) Technical Advisory Board (TAB) established a multi-agency contract vehicle for commercially available, tactical communication equipment and services – the TACCOM II Indefinite Delivery/Indefinite Quantity contract – which was awarded on May 3, 2019. In alignment with the TACCOM II ordering guide and Directive 034-08 *Land Mobile Radio Procurements, Standards, and Specifications*, Components WILL be required to use the TACCOM II IDIQ for procuring equipment and services for Tactical Communications, unless a waiver is procured. Per the approved TACCOM II IDIQ contract, it is a requirement for the WMO to act as a coordination point for collaborative requirements and purchase requests oversight on all DHS-wide TACCOM procurements, providing cost efficiencies with bulk buys whenever possible.

4.1.2 Project 25 (P25) Compliance

P25 also known as Telecommunications Industry Association (TIA)-102, is an LMR standard maintained by the TIA. P25 defines a set of standard functions and interfaces that assure that communications equipment can securely interoperate regardless of vendor.

According to the P25 Technology Interest Group, P25 compliance requires only the Improved Multi-Band Excitation (IMBE) vocoder and the Common Air Interface (CAI). Compliance with these two features does not imply compliance with all the standard functions and interfaces required for security functionality.

Section 4.0 of DHS 4300A requires that all LMR systems comply with P25 security standards. Interoperability between the wireless tactical systems of different DHS Components, as well as those of other state, regional, tribal, territorial and other federal government entities, is essential to the homeland security mission. In situations in which interoperability is necessary for the success of a mission, users will inevitably operate their equipment only at the highest security mode that allows them to interoperate. P25 security standards ensure that security does not have to be sacrificed for interoperability.

4.1.2.a. All procurements SHALL require that applicable wireless tactical system equipment support:

- P25 CAI[1]
- P25 IMBE vocoder[2]
- P25 Advanced Encryption Standard (AES) encryption[3]

4.1.2.b. All procurements SHOULD require that applicable wireless tactical system equipment support:

- P25 Digital Encryption Standard (DES) encryption[4] (to support communications with legacy radios)
- P25 OTAR[5]
- P25 trunking[6]

4.1.3 FIPS PUB 140 Topology Compliance

FIPS 140 specifies security requirements for cryptographic modules used to encrypt SBU information. The standard designates four levels of compliance, Level 1 being the least secure and Level 4 being the most secure.

The overall security level is the minimum of the levels in each area. A list of FIPS PUB 140 topology validated cryptographic modules, along with validation certificates and security

[1]The P25 CAI is specified in ANSI/TIA/EIA 102.BAAA, *Project 25 FDMA Common Air Interface*; TSB102.BAAB-A, *APCO Project 25 Common Air Interface Conformance Test*; ANSI/TIA/EIA 102.BAAC, *Project 25 Common Air Interface Reserved Values*; and TSB102.BAAD, *APCO Project 25 Common Air Interface Operational Description for Conventional Channels*.

[2]The P25 IMBE vocoder is specified in ANSI/TIA/EIA 102.BABA, *Project 25 Vocoder Description*; ANSI/TIA/EIA 102.BABB, *Project 25 Vocoder Mean Opinion Score Conformance Test*; and ANSI/TIA/EIA 102.BABC, *Project 25 Vocoder Reference Test*.

[3]P25-compliant AES is specified in TIA/EIA 102.AAAD, *Block Encryption Protocol*.

[4]P25-compliant DES is specified in TIA/EIA 102.AAAD, *Block Encryption Protocol* and ANSI/TIA/EIA 102.AAAA-A, *P25 DES Encryption Protocol*.

[5]P25-compliant OTAR is specified in ANSI/TIA/EIA 102.AACA, *Project 25 Digital Radio Over-the-Air-Rekeying (OTAR)Protocol*; ANSI/TIA 102.AACB, *Project 25 – Over-the-Air-Rekeying (OTAR) Operational Description*; and ANSI/TIA/EIA 102.AACC, *Conformance Tests for the Project 25 Over-the-Air-Rekeying (OTAR) Protocol*.

[6]P25-compliant trunking is specified in TSB102.AABA, *APCO Project 25 Trunking Overview*; ANSI/TIA/EIA 102.AABB, *Project 25 Trunking Control Channel Formats*; ANSI/TIA/EIA 102.AABC, *Project 25 Trunking Control Channel Messages*; and TSB102.AABD, *Project 25 Link Control Word Formats and Messages*.

policies can be found at https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search. Each cryptographic module's security policy specifies under what modes of operation the module is FIPS validated.

4.1.3.a. All applicable wireless tactical system equipment SHALL have, at a minimum, FIPS PUB 140 topology validated AES cryptographic modules.

4.1.3.b. All applicable wireless tactical system equipment SHOULD be at least Level 2 validated in the roles, services, and authentication area so that it requires role-based or identity-based operator authentication.

4.1.3.c. All applicable wireless tactical system equipment SHOULD be at least Level 3 validated in the physical security area so that it requires tamper detection and response for covers and doors.

4.2 Configuration Requirements

Even if a system meets all the acquisition requirements, it must be properly configured in order to comply with DHS security policy. This section addresses talk group and channel configuration, service minimization, administrative access control, and security auditing.

4.2.1 Talk Group and Channel Configuration

The purpose of talk groups is to ensure that the information being transmitted is only received by the users who need to know it. However, it is possible for a radio to be manually switched to a channel being used by a talk group to which it does not belong. If that radio has the same TEK as the talk group, it can be used to intercept the talk group's communications.

4.2.1.a. Systems administrators of wireless tactical systems SHALL enable FIPS PUB 197 *Advanced Encryption Standard (AES)* 256-bit encryption on all talk groups and channels that support encryption.

4.2.1.b. Each talk group or channel supporting encryption SHALL be configured with a unique TEK.

4.2.2 Additional Connectivity Protocols and Capabilities

Wireless connectivity for ancillary use can be provided through different means. Additional capabilities can be used through Bluetooth and Wi-Fi (802.11) protocols for a data path to LMR subscriber devices and infrastructure equipment. Additional information can be found on specific use of these protocols in DHS 4300A Attachment Q1 - Wireless Systems and Attachment Q6 - Bluetooth Security.

4.2.2a. Management, security measures, and practices SHALL be used for interconnection of LMR subscriber devices and infrastructure equipment using these protocols.

4.2.2b. All LMR subscriber devices and infrastructure equipment SHALL prescribe to encryption standards specified within this directive, as well as DHS 4300A Attachment Q1 and Q6.

4.2.2c. Wi-Fi (802.11) SHALL comply with FIPS PUB 197 AES 256-bit encryption, as prescribed in DHS 4300A Attachment Q1 – Wireless Systems.

4.2.2d. Bluetooth SHALL use the highest-level security mode possible, providing authenticated pairing and encryption using 128-bit strength keys generated using FIPS approved AES encryption as prescribed in DHS 4300A Attachment Q6, and compliance with NIST SP 800-121 *Guide to Bluetooth Security*.

4.2.3 Service Minimization

Wireless tactical systems often have additional built-in features and services that are not necessary for carrying out a Component's mission and that are not covered by security policy. Using these features and services may expose the system to unknown threats.

4.2.3.a. Components SHALL review and evaluate all features and services. Those features or services that are not essential to the operation of the wireless tactical system SHALL be disabled.

4.2.4 Administrative Access Control

Unauthorized access to a wireless tactical system's administrative controls would pose a serious threat to the security of the system.

4.2.4.a. The wireless tactical system SHALL be configured to require strong authentication in order to grant access to administrative controls. The authentication SHALL include a username and password.

4.2.4.b. The manufacturer or any other vendor SHALL not have control over the administrative password. Hard coded and permanent passwords SHALL not be permitted.

4.2.5 Security Auditing

DHS 4300A requires that audit trails shall be sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. The ability to audit the actions of a user of a system, along with the use of individually assigned authentication controls, provides accountability. Audit records provide security managers with a means to detect misuse or intrusion, identify exposed sensitive data, and, in some cases, track the source of the security breach.

4.2.5.a. The wireless tactical system SHALL be configured to create, maintain, and protect an audit trail, including the following security-related events, to the extent the technology supports this capability:

- Key transactions;
  - Key zeroization requests (successful and failed)
  - Rekeying requests (successful and failed)
- Key management message (KMM) failures;
  - Message authentication code (MAC) failures
  - Message number (MN) failures
- Deactivation of a security feature;
- Successful and unsuccessful logins; and;
- Access to system administrator functions.

4.3 Fault Tolerance

To ensure the availability of critical systems, those supporting security functionality, organizations build redundancies through their wireless tactical systems so that if a system component fails, a backup exists to continue operations.

4.3.a. DHS components SHALL procure, implement, and maintain a backup KMF for each wireless tactical system that uses a KMF. The backup SHOULD be located at an alternate site and support the same capabilities and capacity as the primary KMF.

4.4 Legacy Migration Requirements

Section DHS 4.0 of 4300A requires the migration of legacy wireless tactical systems to DHS IT security policy compliance. Components must create migration plans for noncompliant systems outlining the provisions, procedures, and restrictions for transitioning these systems to DHS-compliant security architectures. One important provision of these plans is to ensure secure interoperability between new systems and legacy systems during transition activity.

4.4.a. Legacy migration plans SHOULD ensure that new systems and legacy systems share at least one cryptosystem standard so that they can interoperate without disabling message encryption.

4.5 Future Developments

LMR technology is constantly evolving. Future developments will likely include guidance for the following:

- Implementation of phases II and III of P25;
- FIPS 140topology compliance;
- NextGen technologies to include mobile applications compliant with 3rd Generation Partnership Project (3GPP) standards;
- Secure P2P communication;
- Secure over-the-air programming and zeroization; and
- Audit capabilities and centralized audit management.

5.0 TRAINING AND EXERCISES

Proper training and regular exercises are critical to maintaining OPSEC. The key objective of security training is to ensure that each employee understands the security implications of his/her actions and is educated regarding the Component's and department security policies and procedures, to include reference to this document. Security training includes both security awareness and technical training courses. Operational exercises reinforce the lessons learned and give employees an opportunity to put their training into practice.

5.1 Security Awareness Training

A Component cannot ensure the security of its wireless tactical system without the knowledge and active participation of its employees in the implementation of sound security principles.

5.1.a. Components are reminded that DHS 4300A requires that appropriate awareness training SHALL be provided and SHOULD include information pertinent to security methods used with mission critical voice systems and end units.

5.1.b. Any appropriate wireless security awareness training SHOULD be included in the annual training provided at the Component level.

5.1.c. Upon completion of the security awareness training for wireless tactical systems, a system user SHOULD, at a minimum, have knowledge of the following:

- The Component's security policy and SOPs related to the wireless tactical system
- The following radio frequency (RF) communication threats, the measures taken to counter them, and the means for detecting their occurrence:
  - Message interception
  - Data intercept/replay
  - Voice Intercept/replay
  - Spoofing
  - Misdirection
  - Jamming
  - Traffic analysis
  - Subscriber duplication
  - Theft of service
- How to identify, respond to, and report security incidents, including:
  - Lost or stolen radio
  - Key compromise
  - Radio frequency interference
  - Broken or tampered-with radio
  - Any of the threats in the preceding item

5.2 Operator Training

In addition to the security awareness training required by DHS 4300A, before being given access to the wireless tactical system, each system user must have specific knowledge to operate LMR subscriber devices and infrastructure equipment in compliance with security policies and procedures. Conventional[7] and trunked[8] radios operate differently and require different training. Operator training should align to the baseline Component created training plans in alignment with Directive 034-04 *Joint Wireless Interoperability Program Tactical Communications*. Any updates to these training plans should be coordinated through the WMO.

5.2.a. Each system user's technical training SHALL include hands-on, or virtual refresher, instruction on how to operate the equipment assigned to him/her within the context of his/her roles and responsibilities, and references/provides access to all related SOPs developed by a Component in support of their LMR operations.

[7] "Conventional" implies non-trunked radio communications in which RF channels are manually selected.

[8] "Trunked" implies a computer-controlled communications system, which automatically allocates an RF channel for a call, and at the end of that call, releases the channel so that it can be reallocated for another call.

5.2.b. Components SHALL ensure that newly hired employees have obtained initial technical training prior to giving them access to the wireless tactical systems.

5.2.c. Technical training courses for system users and system administrators SHALL include security-related instructions.

5.2.d. All technical training related to the wireless tactical systems SHALL include material on how to manage and operate LMR subscriber devices and infrastructure equipment, and wireless devices, including add on accessories, such as headsets, in a secure manner.

5.2.e. Security technical training MAY be combined with other technical training related to the wireless tactical system.

5.2.f. Components SHALL include training materials as part of their accreditation package.

5.3 Future Developments

It is imperative that DHS Components and state, regional, tribal, territorial and other federal government entities can interoperate in an encrypted environment using a shared key in response to natural disasters and terrorist attacks and when supporting large-scale planned events. Technologies to support key sharing include the P25 inter-subsystem interface. Future developments with respect to operational exercises might involve this and other key sharing technologies. For example, the possibility exists that public key infrastructure might be used to support key management, which would necessitate training and exercises to ensure its proper implementation.

6.0 USAGE

Usage refers to the implementation of the security controls listed in the previous sections of this document. Successful usage depends on progress in each of these areas as well as the interplay among them. The long-term objective is that all wireless tactical systems at DHS will support robust security mechanisms without adversely impacting the related goal of interoperability.

It is recognized that this document primarily addresses LMR. Guidance on other wireless tactical systems technology is forthcoming.

6.0.a. DHS Components MAY limit the applicability of the security, technical and operational requirements listed in this document to their LMR systems only.

6.0.b. Effective immediately, DHS Components SHALL adhere to the acquisition requirements listed in this document.

6.0.c. DHS Components SHALL continue to fully implement all technical and policy requirements stated within this document.

Appendix A: *References*

APPENDIX A: REFERENCES

Department of Defense, *Test Method Standard for Environmental Engineering Considerations and Laboratory Tests (MIL-STD-810F)*, January 2000.

Department of Homeland Security Management *Directive* 140-01, *Information Technology System Security Program*, Revision 2, May 5, 2017.

Department of Homeland Security Management Directive 034-08, *Land Mobile Radio Procurements, Standards, and Specifications*, October 29, 2019.

Department of Homeland Security, 4300A, *Information Technology System Security Program, Sensitive Systems v1.0, xx/xx/2022*.

National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (SP 800-37 Rev. 2)*, December 2018.

National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules (FIPS PUB 140-2)*, May 2001.

National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules (FIPS PUB 140-3)*, March 2019.

National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199)*, February 2004.

Telecommunications Industry Association, *APCO Project 25 System and Standards Definition (TSB102-A Revision D)*, March 2020.

Telecommunications Industry Association, *APCO Project 25 Trunking Overview (TSB102.AABA Revision C)*, November 2019.

Telecommunications Industry Association, *Digital Land Mobile Radio, Security Services Overview (ANSI/TIA 102.AAAB Revision B)*, February 2019.

Telecommunications Industry Association, *Project 25 Block Encryption Protocol (ANSI/TIA/EIA 102.AAAD Revision B)*, November 2015.

Telecommunications Industry Association, *Project 25 Digital Radio Over-the-Air-Rekeying (OTAR) Protocol (ANSI/TIA/EIA 102.AACA Revision A)*, September 2014.

Telecommunications Industry Association, *Project 25 FDMA Common Air Interface (ANSI/TIA/EIA 102.BAAA Revision B)*, June 2017.

Telecommunications Industry Association, *Project 25 Vocoder Description (ANSI/TIA/EIA 102.BABA Revision A)*, January 2014.

Online References

Bradner, S., *Request for Comments 2119: Key words for Use in RFCs to Indicate Requirement Levels*, http://www.ietf.org/rfc/rfc2119.txt, viewed in July 2021.

Department of Homeland Security, *SAFECOM Interoperability Continuum*, https://www.cisa.gov/safecom/resources, viewed in July 2021.

National Institute of Standards and Technology, *FIPS 140-1 and FIPS 140-2 Cryptographic Modules Validation List*, https://csrc.nist.gov/projects/cryptographic-module-validation, viewed in July 2021.

P25 Technology Interest Group, http://www.project25.org, viewed in July 2021.

Appendix B: *Checklist for Securing Wireless Tactical Systems*

APPENDIX B: CHECKLIST FOR SECURING WIRELESS TACTICAL SYSTEMS

Mobile Feature/Configuration	Required	Recommended
3.0 STANDARD OPERATING PROCEDURES		
3.0.a. Each component SHALL maintain SOPs for each of the following areas: • Key Management • Configuration Management • Security Incident Response • Temporary Suspension of Security Controls • Continuity of Operations Plan (COOP). • Radio over Internet Protocol (RoIP) Network Patching	X	
3.0.b. Each Component MAY maintain separate SOPs for different organizational elements (e.g., divisions, branches, or, in some cases, job categories), if every organizational element is covered by compliant SOPs.		X
3.0.c. Each Component SHALL submit its SOPs to the WMO so that it can review the SOPs' security procedures and requirements for compliance with DHS 4300A.	X	
3.0.d. Components SHALL include minimum departmental standards in each applicable SOP.	X	
3.0.e. A Component MAY exceed a minimum departmental standard, thereby providing additional cybersecurity, if it determines that a higher standard is required to fulfill its mission.		X
3.0.f. SOPs SHALL include the following: • Date and version of the SOP; • Letter of approval/review from the WMO; • Contact information for security-related questions about the SOP; and • Any standard DHS notices or warnings.	X	
3.1.1 Key Generation		
3.1.1.a. The Key Management SOP SHALL identify either (1) the specific hardware and software authorized for key generation or (2) the external entity authorized to provide keys. All key management hardware and infrastructure SHALL be compatible and provide and process the latest specified key configurations and key length provided by NIST and NSA Standards.	X	
3.1.1.b. When an organization generates its own keys, the Key Management SOP SHALL specify the personnel or roles authorized to operate and administer key generation technology and the responsibilities of those personnel or roles.	X	
3.1.1.c. All personnel authorized to generate keys SHOULD be trained in the proper generation and handling of the keys, including the requirement for secrecy.		X

Mobile Feature/Configuration	Required	Recommended
3.1.1.d. If keys from external entities are required for interoperability purposes in the communication of SBU information, then the Component SHALL receive approval from the CISO before using such keys.	X	
3.1.1.e. If SBU keys are obtained from an external entity other than the NSA to support interoperability, then the Key Management SOP SHALL: • Specify the persons or roles permitted to receive keys and handle key material; • Require that the person receiving a key record the date and time the key was received and the name and affiliation of the person from which the key was received; and • Implement a process by which someone can trace each externally supplied key in use to its source.	X	
3.1.2 Key Distribution		
3.1.2.a. The Key Management SOP SHALL specify the chosen authorized methods for key distribution.	X	
3.1.2.b. The specified method SHALL either involve out-of-band distribution or encryption of keys prior to distribution.	X	
3.1.2.c. All key distribution transactions SHALL be logged. The log records SHALL be protected against unauthorized modification and retained for a period of at least one (1) year.	X	
3.1.3 Key Storage		
3.1.3.a. Keys SHALL be stored in an encrypted format.	X	
3.1.3.b. The Key Management SOP SHALL specify the authorized locations in which keys are permitted to be stored.	X	
3.1.3.c. Keys that are removable from LMR subscriber devices and infrastructure equipment, such as keys stored on tokens or hard copy versions of keys, SHALL be physically secured when not in use.	X	
3.1.3.c. The physical security SHOULD be in accordance with DHS 4300A, *Information Technology System Security Program,Sensitive System's"* General Physical Access policy and DHS IT Security Architecture Guidance Volume II: Security Operations and Support policy.		X
3.1.4 Key Destruction		
3.1.4.a. The Key Management SOP SHALL specify the procedure to sanitize storage media containing key material after it is no longer required for operations	X	
3.1.4.b. The sanitization procedure SHOULD involve technology other than simple file deletion. It MAY involve degaussing magnetic media, using disk-wiping utilities, over-the-air zeroization, or physical media destruction.		X
3.1.4.c. Key material stored in a hard copy format SHALL be either shredded, burned, or pulped when that key is no longer required to support operations.	X	
3.1.5 Suspected Key Compromise		

Mobile Feature/Configuration	Required	Recommended
3.1.5.a. The Security Incident Response SOP SHALL instruct any person suspecting a key compromise to report it immediately	X	
3.1.5.b. The Security Incident Response SOP SHALL specify to whom the suspected key compromise reporting should be directed.	X	
3.1.5.b …This person SHOULD be a security operations center or on-call security operations personnel.		X
3.1.5.c. The recipient of a suspected key compromise report SHOULD notify the Component Information System Security Officer (ISSO) as soon as practicable. This notification MAY NOT be immediate if the original report was received outside of business hours.		X
3.1.5.d. The Security Incident Response SOP SHALL specify the options for communicating suspected key compromise. These options SHALL include both telephone and e-mail.	X	
3.1.5.e. The Security Incident Response SOP SHALL specify a verbal code to use when performing in-band reporting of a suspected compromise.	X	
3.1.5.e. … Such reporting MAY be necessary during a tactical operation if alternative means of communication are unavailable but SHOULD NOT be used if alternative means are available.		X
3.1.5.f. The Security Incident Response SOP SHALL specify the process for determining when a report of a suspected compromise warrants a response.	X	
3.1.5.f. … The process SHOULD anticipate the need for a response within 4 hours. It MAY involve an order from the ISSO, or systems operations personnel MAY be given authority to act without approval under special circumstances to be specified in the SOP.		X
3.1.5.g. If it is determined that a response to a suspected key compromise warrants a response, the response SHALL include rekey of any such key on all devices that possess the key.	X	
3.1.6 Periodic Rekeying		
3.1.6.a. The Key Management SOP SHALL specify the frequency of key replacement for Component traffic encryption keys (TEK)…	X	
3.1.6.a. …and SHOULD not exceed a 30-day key cycle.		X
3.1.6.a. Key cycles exceeding 30 days SHALL require a waiver from the DHS CISO, with WMO review and concurrence. A waiver MUST be based on mission essential requirements and justification for extended key cycles. Waivers SHALL not authorize more than a 180-day key cycles.	X	
3.1.6.b. Key Encryption Keys (KEKs) that are shared across multiple LMR subscriber devices and/or infrastructure equipment SHOULD be replaced periodically.	X	
3.1.6.b. … KEKs that uniquely identify a particular LMR subscriber device and/or infrastructure equipment MAY be kept in service indefinitely.		X
3.2 Configuration Management		
3.2.a. Each Component SHALL maintain documentation on the encryption configuration state of each wireless tactical system it operates.	X	

Mobile Feature/Configuration	Required	Recommended
3.2.b. Each Component SHALL establish a written change approval process for each wireless tactical system it operates.	X	
3.2.c. The Configuration Management SOP SHALL specify the membership of the Configuration Control Board (CCB).	X	
3.2.c. … The CCB membership SHOULD be based on personnel roles rather than named individuals		X
3.2.d. The Configuration Management SOP SHALL specify the procedure by which each proposed change SHALL be brought before the CCB for approval. The procedure SHOULD include a description of the information that must accompany each change request (CR). The CR information SHALL at a minimum include the following: • The purpose of the change; • The specific equipment or systems that the change will impact; • The date and time the change will be performed; • The duration of the work; • Whether the change is expected to cause a temporary outage or performance degradation; • The personnel who will be performing the change; and • The rollback procedure in case the change does not have its intended effect.	X	
3.2.e. The Configuration Management SOP SHALL specify the voting procedure for CR approval.	X	
3.2.e. … Approval SHOULD require unanimous written consent of the CCB membership. Written consent MAY be electronic, such as through an e-mail message or an authenticated entry in a configuration management software tool		X
3.2.f. The Configuration Management SOP SHALL specify an emergency change procedure for any configuration changes that needs to occur prior to a meeting of the CCB in order to restore the availability or security of the system.	X	
3.2.g. The Configuration Management SOP SHALL require timely submission of an emergency CR for retroactive approval of each emergency change.	X	
3.2.g. … The time frame for submission of an emergency CR SHOULD be no longer than 48 hours after the change. The configuration management SOP SHOULD require that the system be rolled back to its state prior to the emergency whenever an emergency CR is not approved.		X
3.2.h. The Configuration Management SOP SHOULD include controls related to the appropriate separation of duties. Individuals who develop software, scripts, or radio programming instructions SHOULD NOT be permitted to implement the software, scripts or instructions on operational systems.	X	

Mobile Feature/Configuration	Required	Recommended
3.2.i. The Configuration Management SOP SHALL specify the procedure by which technical personnel document the completion of an approved CR. The procedure SHOULD include a description of the information that must accompany each after-action report (AR). The AR information SHOULD include the following: • Who performed the work specified in the CR; • Whether the work was performed successfully; • If the work was not performed successfully, whether the rollback procedure was performed successfully; • Whether any steps had to be added or removed to achieve the desired result; and • The date and time the work was started and finished.	X	
3.2.j. Retirement or disposal of system hardware SHALL be considered a configuration change. The Configuration Management SOP SHALL specify the procedure for sanitizing media of key material and other sensitive data prior to disposal. The authorized techniques SHALL NOT include simple file deletion. They may include zeroization or degaussing	X	
3.2.k. The Configuration Management SOP SHALL specify the recordkeeping requirements of CCB proceedings. Approved CRs and approved ARs SHALL be maintained for a period of not less than one (1) year.	X	
3.2.k. … They SHOULD be maintained for the operational lifetime of the system.		X
3.3 Security Incident Response		
3.3.a. The Security Incident Response SOP SHALL specify methods for communication device users and other personnel to report security incidents, in accordance with DHS 4300A, Instructions F. One of the methods SHALL be via a telephone call to a security operations center or on-call security operations personnel.	X	
3.3.b. The security incident response capability SHOULD be available on a continuous basis (i.e., 24 hours a day, 365 days a year).		X
3.3.c. Each security incident report SHOULD include the following: • Equipment or technology involved (i.e., make, model, etc.); • Event (e.g., loss, theft, no longer operational); • Personnel involved; • Location of incident; • Circumstances of incident; • Possibility of compromise; and • Point of contact.		X
3.3.1 Lost or Stolen LMR Subscriber Device		
3.3.1.a. The Security Incident Response SOP SHALL specify the procedure that SHALL be followed to report a lost, stolen, malfunctioning, or tampered-with LMR subscriber device. The procedure SHALL specify that such reporting occur immediately or as soon as it is feasible to do so.	X	

Mobile Feature/Configuration	Required	Recommended
3.3.1.b. The Security Incident Response SOP SHALL specify the actions that a systems administrator and owner SHALL take in response to notification of a lost, stolen, malfunctioning, or tampered-with LMR subscriber device. These actions SHALL include preventing the LMR subscriber device from authenticating to the LMR network or participating in a talk group.	X	
3.3.1.b The actions SHOULD include rekeying all LMR subscriber devices holding the same TEKs as the lost, stolen, malfunctioning, or tampered-with LMR subscriber device. The actions SHOULD include over-the-air zeroization of key material if this feature is available.		X
3.3.2 Radio Frequency Interference		

3.3.2.a. The Security Incident Response SOP SHALL specify the actions to take after radio users detect radio interference. The actions SHALL at a minimum include:
• Notifying a relevant authority that the interference is occurring
  o The first authority should be within the Component and associated stakeholders
  o If interference continues, contact the WMO Spectrum Management Team to assist.
• Mitigating the impact of the interference
	X	

3.3.2.b. The first technical approach to interference impact mitigation SHOULD be to change frequencies, if the radio technology supports this approach.		X
3.3.2.c. If radio interference is expected or is common that cannot be circumvented through changing the frequency, then tactical personnel SHOULD have the ability to switch to a backup form of wireless communications. The backup MAY be the use of a commercial cellular telephone.		X
3.3.2.d. The security Incident Response SOP MAY cover procedures for the identification of the source of interference through triangulation or other means. If such procedures are included, they SHOULD include methods of evidence collection that would allow for subsequent prosecution of illegal behavior.		X
3.4 Temporary Suspension of Security Controls		
3.4.a. The Temporary Suspension of Security Controls SOP SHALL specify the roles that are authorized to permit the temporary suspension of security controls. The authorized roles SHALL NOT include LMR subscriber device users. They MAY include an incident commander, system owner, or ISSO.	X	
3.4.b. The Temporary Suspension of Security Controls SOP SHALL specify the conditions under which override is permitted. These conditions SHALL include (1) critical communication cannot occur without override and (2) delay MAY lead to a significant adverse consequence.	X	
3.4.c. Temporary suspension of controls SHALL NOT be invoked to support interoperability unless it is determined that there is no means to bridge communications. Bridge communications options MAY include the use of special technology designed for that purpose or selecting personnel to hold multiple LMR subscriber devices.	X	

Mobile Feature/Configuration	Required	Recommended
3.4.d. The system's Authorizing Official (AO) (Note: Authorizing Official replaces the term Designated Accrediting Authority (DAA) as per NIST SP 800-37) and ISSO SHALL be notified as soon as practicable whenever security controls are temporarily suspended.	X	
3.5 Continuity of Operations Planning		
3.5.a. The COOP SOP SHALL specify the roles and responsibilities of personnel during a significant system outage. A personnel notification roster SHOULD be distributed among all relevant personnel for use during emergencies or significant outages	X	
3.5.b. The COOP SOP SHALL specify the circumstances under which personnel should operate LMR subscriber devices in ad hoc or P2P mode (e.g., when infrastructure connectivity is unavailable).	X	
3.5.c. The COOP SOP SHALL list other authorized mechanisms for receiving and transmitting information when tactical systems are unavailable. Such mechanisms MAY include the use of commercial cellular telephones or, for broadcast purposes, broadcast radio or Internet websites.	X	
3.6 Radio Centric IT infrastructure Systems and Network Patching		
3.6.a. Components SHALL develop and maintain a Configuration Management SOP, to include patching and implementing updates to system components and infrastructure. The SOP SHALL specify methods, processes, and requirements for these actions.	X	
3.6.b. Components SHALL perform vulnerability scans on supported test systems using third-party scanning tools to identify and address new vulnerabilities and compliance issues.	X	
3.6.c. Configuration management policies MUST include provisions for quickly testing and approving time-sensitive changes that result from newly released vulnerability information.	X	
3.6.d. Patches and updates SHOULD be implemented once tested and validated	X	
3.6.e. Components SHALL monitor for and obtain alerts from CISA, DHS CISO, Information Assurance Vulnerability Management (IAVM) alerts issued by the DoD Computer Emergency Response Center (DoD-CERT), and Original Equipment Manufacturer (OEM) Bulletins and updates as appropriate.	X	
4.0 Technology		
4.1.2 P25 Compliance		
4.1.2.a. All procurements SHALL require that applicable wireless tactical system equipment support: • P25 CAI • P25 IMBE vocoder • P25 Advanced Encryption Standard (AES) encryption	X	

Mobile Feature/Configuration	Required	Recommended
4.1.2.b. All procurements SHOULD require that applicable wireless tactical system equipment support: • P25 Digital Encryption Standard (DES) encryption (to support communications with legacy radios) • P25 OTAR • P25 trunking		X
4.1.3 FIPS 140 Topology Compliance		
4.1.3.a. All applicable wireless tactical system equipment SHALL have, at a minimum, FIPS PUB 140 topology validated AES cryptographic modules.	X	
4.1.3.b. All applicable wireless tactical system equipment SHOULD be at least level 2 validated in the roles, services, and authentication area so that it requires role-based or identity-based operator authentication.		X
4.1.3.c. All applicable wireless tactical system equipment SHOULD be at least level 3 validated in the physical security area so that it requires tamper detection and response for covers and doors.		X
4.2.1 Talk Group and Channel Configuration		
4.2.1.a. Systems administrators of wireless tactical systems SHALL enable FIPS PUB 197 *Advanced Encryption Standard* (AES) 256-bit encryption on all talk groups and channels that support encryption.	X	
4.2.1.b. Each talk group or channel supporting encryption SHALL be configured with a unique TEK.	X	
4.2.2 Additional Connectivity Protocols and Capabilities		
4.2.2a. Management, security measures, and practices SHALL be used for interconnection of LMR subscriber devices and infrastructure equipment using these protocols.	X	
4.2.2b. All LMR subscriber devices and infrastructure equipment SHALL prescribe to encryption standards specified within this directive, as well as DHS 4300A Attachment Q1 and Q6.	X	
4.2.2c. Wi-Fi (802.11) SHALL comply with FIPS PUB 197 AES 256-bit encryption, as prescribed in DHS 4300A Attachment Q1 – Wireless Systems.	X	
4.2.2d. Bluetooth SHALL use the highest-level security mode possible, providing authenticated pairing and encryption using 128-bit strength keys generated using FIPS approved AES encryption as prescribed in DHS 4300A Attachment Q6, and compliance with NIST SP 800-121Guide to Bluetooth Security.	X	
4.2.3 Service Minimization		
4.2.3.a. Components SHALL review and evaluate all features and services. Those features or services that are not essential to the operation of the wireless tactical system SHALL be disabled.	X	
4.2.4 Administrative Access Control		

Mobile Feature/Configuration	Required	Recommended
4.2.4.a. The wireless tactical system SHALL be configured to require strong authentication in order to grant access to administrative controls. The authentication SHOULDSHALL include a username and password.	X	
4.2.5 Security Auditing		

4.2.5.a. The wireless tactical system SHALL be configured to create, maintain, and protect an audit trail, including the following security-related events, to the extent the technology supports this capability:
• Key transactions
  o Key zeroization requests (successful and failed)
  o Rekeying requests (successful and failed)
• Key management message (KMM) failures
  o Message authentication code (MAC) failures
  o Message number (MN) failures
• Deactivation of a security feature
• Successful and unsuccessful logins
• Access to system administrator functions.
	X	

4.3 Fault Tolerance		
4.3.a. DHS components SHALL procure, implement, and maintain a backup KMF for each wireless tactical system that uses a KMF.	X	
4.3.b … The backup SHOULD be located at an alternate site and support the same capabilities and capacity as the primary KMF.		X
4.4 Legacy Migration Requirements		
4.4.a. Legacy migration plans SHOULD ensure that new systems and legacy systems share at least one cryptosystem standard so that they can interoperate without disabling message encryption.		X
5.0 TRAINING AND EXERCISES		
5.1 Security Awareness Training		
5.1.a. Components are reminded that DHS 4300A requires that appropriate awareness training SHALL be provided and should include information pertinent to security methods used with mission critical voice systems and end units.	X	
5.1.b. Any appropriate wireless security awareness training SHOULD be included in the annual training provided at the Component level.		X

Mobile Feature/Configuration	Required	Recommended
5.1.cc. Upon completion of the security awareness training for wireless tactical systems, a system user SHOULD, at a minimum, have knowledge of the following: • The Component's security policy and SOPs related to the wireless tactical system • The following radio frequency (RF) communication threats, the measures taken to counter them, and the means for detecting their occurrence: o Message interception o Data intercept/replay o Voice Intercept/replay o Spoofing o Misdirection o Jamming o Traffic analysis o Subscriber duplication o Theft of service • How to identify, respond to, and report security incidents, including: o Lost or stolen radio o Key compromise o Radio frequency interference o Broken or tampered-with radio o Any of the threats in the preceding item		X
5.2 Technical Training		
5.2.a. Each system user's technical training SHALL include hands-on, or virtual refresher, instruction on how to operate the equipment assigned to him/her within the context of his/her roles and responsibilities, and references/provides access to all related SOPs developed by a Component in support of their LMR operations.	X	
5.2.b. Components SHALL ensure that newly hired employees have obtained initial technical training prior to giving them access to the wireless tactical systems.	X	
5.2.c. Technical training courses for system users and administrators SHALL include security-related instructions.	X	
5.2.d. All technical training related to the wireless tactical systems SHALL include material on how to manage and operate LMR subscriber devices and infrastructure equipment, and wireless devices, including add on accessories, such as headsets, in a secure manner.	X	
5.2.e. Security technical training MAY be combined with other technical training related to the wireless tactical system.		X
5.2.e. Components SHALL include training materials as part of their accreditation package	X	

Mobile Feature/Configuration	Required	Recommended
6.0 USAGE		
6.0.a. DHS Components MAY limit the applicability of the security, technical and operational requirements listed in this document to their LMR systems only.	X	
6.0.b. Effective immediately, DHS Components SHALL adhere to the acquisition requirements listed in this document.	X	
6.0.cc. DHS Components SHALL continue to fully implement all technical and policy requirements stated within this document.	X	

Appendix C: *Physical and Environmental Security*

APPENDIX C: PHYSICAL AND ENVIRONMENTAL SECURITY

The following controls SHOULD be considered to protect the wireless tactical system infrastructure from physical and environmental threats.

- Facility security
  - Fenced perimeters
  - Visitor log
  - Visitor escort
  - Electronic access devices
  - Security cameras
  - Alarmed doors
- Computer room security
  - Visitor's log
  - Visitor escort
  - Key locks
  - Cipher lock
  - Electronic access devices
  - Alarmed doors
- Telecommunications closet security
  - Key locks
  - Cipher locks
- Remote tower sites security
  - Fenced perimeters
  - Barbed wire
  - Visitor log
  - Visitor escort
  - Key locks
  - Cipher locks
  - Electronic access devices
  - Security cameras
  - Alarmed doors
- Environmental protection
  - Fire extinguishers
  - Fire suppression systems
  - Smoke detectors
  - Fire sprinklers
  - Fire alarm system
  - Lightning protection
  - Uninterruptible power supplies (UPS)
  - Batteries
  - Generators
  - Independent air conditioning units
  - Raised floors
  - Emergency lighting
  - Surge protectors

Appendix D: *Acronyms*

APPENDIX D: ACRONYMS

AES	Advanced Encryption Standard
AO	Authorizing Official
AR	After-action Report
C&A	Certification and Accreditation
CAI	Common Air Interface
CCB	Change Control Board
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COOP	Continuity of Operations Plan
CR	Change Request
DAA	Designated Approving Authority
DES	Data Encryption Standard
DHS	Department of Homeland Security
DoD	Department of Defense
FIPS	Federal Information Processing Standard
HF	High Frequency
IA	Information Assurance
IA	Information Assurance
IETF	Internet Engineering Task Force
IMBE	Improved Multi-Band Excitation
ISSO	Information System Security Officer
IT	Information Technology
KEK	Key Encryption Key
KMF	Key Management Facility
KMM	Key Management Message
KVL	Key Variable Loader
LMR	Land Mobile Radio
MAC	Message Authentication Code
MN	Message Number
NIST	National Institute of Standards and Technology
NSA	National Security Agency

OPSEC	Operations Security
OTAR	Over-The-Air Rekeying
P25	Project 25
RF	Radio Frequency
SOP	Standard Operating Procedure
SP	Special Publication
TAB	Technical Advisory Board
TACCOM	Tactical Communication
TEK	Traffic Encryption Key
TIA	Telecommunications Industry Association
VHF	Very High Frequency
WMO	Wireless Management Office
WSB	Wireless Security Board