U.S. Customs and Border Protection

Attachment Q3

Sensitive Wireless Tactical Systems

HB 1400-05D
Information Systems Security Policies and Procedures Handbook

Version 2.0

July 27, 2009

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	July 27, 2009	Initial CBP 1400-05D release based solely on DHS 4300A, Version 6.1.1, attachment. There are no substantive differences between this CBP attachment and its source DHS attachment. This attachment is included as part of the CBP 1400-05D handbook suite to enable the CBP user to be able to access all IT security policies (DHS as well as CBP specific) at one location.
2.0	December 21, 2010	Introduced new terminology Authorizing Official (AO) – replaces DAA, as per NIST 800-37 and 800-53

CONTENTS

1.0 INTRODUCTION

This document provides requirements and guidance to assist Customs and Border Protection (CBP) in the development and implementation of their information assurance (IA) programs for their wireless tactical systems. It is a supplement to the CBP Information Systems Security Policies and Procedures Handbook, 1400-05D and is intended to be read in conjunction with that document, especially Section 4.0,. Within Attachment Q3, the use of the word "shall" shall be considered mandatory only in as it applies to existing CBP policy elements. Attachment Q3 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 CBP wireless security policy beyond CBP 1400-05D 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 CBP is required to implement and with which they are expected to monitor compliance. It also suggests best practices and options that CBP should consider when managing it's wireless tactical systems.

1.2 Scope

This document addresses the IA 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), 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 CBP Chief Information Officer (CIO) through the CBP Chief Information Security Officer (CISO). For topics not covered in the CBP 1400-05D compilation (which includes this document as well as other supplements to CBP 1400-05D, departmental directives shall remain in effect until relevant CBP policy and implementing guidance are issued.

1.4 Wireless Tactical Systems

Wireless tactical systems include LMR subscriber devices and infrastructure equipment, Marine VHF FM radio subscribers, HF voice and data devices and infrastructure equipment, remote sensors, and technical investigative communications systems. Because they are often deployed under circumstances in which officer safety and mission success are at stake, wireless tactical systems require even greater security measures than those employed with other wireless communications technologies. To ensure encrypted tactical communications, CBP must implement strong identification, authentication, and encryption protocols designed specifically for each wireless tactical system. The following policy is found in Section 4.6.3 of the CBP Information Systems Security Policies and Procedures.

CBP Policy
a. The AO 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.
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. A current inventory of all approved wireless tactical systems in operation shall be maintained.
e. Legacy tactical wireless systems that are not compliant with CBP IT security policy shall implement a migration plan to outline the provisions, procedures, and restrictions for transitioning these systems to CBP-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception from the DHS and/or CBP CISO, as appropriate.
f. The security configuration of Land Mobile Radio (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 Handbook

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 CBP 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 in particular, 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, which is 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 IA mechanisms because of a concern that they could impede interoperability. Integrating IA requirements into an interoperability framework helps alleviate this concern because it demonstrates the potential synergy between IA and interoperability.

1.6 Revisions to the Handbook

The WMO publishes this handbook 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 CBP 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.

2.1 Wireless Management Office

The WMO, a component of the office of the DHS 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.
- Sharing of governance best practices across DHS so that CBP can improve its internal governance of wireless tactical systems.
- Development of governance structures involving organizations outside of DHS in order to support interoperability of communication between CBP.

3.0 STANDARD OPERATING PROCEDURES

Operations security (OPSEC) is a critical component of IA. 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. CBP SHALL maintain SOPs for each of the following areas:

- Key management

- Configuration management
- Security incident response
- Temporary suspension of security controls
- Continuity of operations (COOP).

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

3.0.c. CBP SHALL submit its SOPs to the WMO so that it can review the SOPs' security procedures and requirements for compliance with CBP 1400-05D.

The remainder of this section explains the content of each SOP in more detail. CBP 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. CBP SHALL include minimum departmental standards in each applicable SOP.

3.0.e. CBP MAY exceed a minimum departmental standard, thereby providing additional IA, 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
- Contact information for security-related questions about the SOP
- Any standard CBP notices or warnings.

3.1 Key Management

Cryptographic keys are required to adequately support IA 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.

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 particular 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 CBP SHALL receive approval from the CBP 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
- 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 in order for encrypted communications to occur. If secret keys are revealed during the distribution process, the security properties of the cryptosystem are lost. To help ensure secrecy 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 radio to a key variable loader (KVL). Another method to distribute keys is over-the-air rekeying (OTAR), typically using a wireless connection between the radio and a KMF. OTAR provides centralized key management and can quickly distribute keys to many radios 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 1 year.

3.1.3 Key Storage

Keys must be kept at their same classification level during storage as well as distribution. All radios 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 radio devices, 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 CBP Information Systems Security Policies and Procedures Handbook, 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 still 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 or burned 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 radio, 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 a radio 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 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 4 hours. It MAY involve an order from the ISSO, or systems operations personnel MAY be given authority to take action 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 radios have the same key; if any radios 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 traffic encryption keys (TEK), which is not to exceed 30 days.

3.1.6.b. KEKs that are shared across multiple radios SHALL be replaced at the same frequency as TEKs. KEKs that uniquely identify a particular radio 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. CBP SHALL maintain documentation on the encryption configuration state of each wireless tactical system it operates.

3.2.b. CBP 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
- 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
- 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 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 security 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 radio users and other personnel to report security incidents, in accordance with CBP 1400-05D, Attachment F. One of the methods SHALL be via a telephone call to a 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
- Point of contact.

3.3.1 Lost or Stolen Radio

If an adversary either steals a radio or obtains a lost radio, then the adversary can listen to or participate in sensitive communications. A malfunctioning or tampered-with radio 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 radio. 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 radio. These actions SHALL include preventing the radio from authenticating to the radio network or participating in talk group. The actions SHOULD include rekeying all radios holding the same TEKs as the lost, stolen, malfunctioning, or tampered-with radio. 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.

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
- Mitigating the impact of the interference.

3.3.2.b. The first technical approach to interference impact mitigation SHOULD be to change frequencies, as long as 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 SOP SHALL specify the roles that are authorized to permit the temporary suspension of security controls. The authorized roles SHALL NOT include radio users. They MAY include an incident commander, system owner, or ISSO.

3.4.b. The temporary suspension 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 radios.

3.4.d. The system's Authorizing Official (AO) 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 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 radios in ad hoc or peer-to-peer 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 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 CBP or federal agencies, or between CBP and state and local organizations supporting tactical operations
- SOPs to support the creation, use, and break-down of ad hoc or peer-to-peer networks when centralized infrastructure is unavailable or for any other reason
- Improved guidance on identifying and avoiding radio interference
- Technology-specific guidance providing step-by-step instructions on how to implement security controls on a particular make and model of a radio or its supporting equipment
- Guidance related to the development of system specific Rules of Behavior, in accordance with CBP 1400-05D, Attachment G.

4.0 TECHNOLOGY

Properly configured technology is a critical component of IA. This section covers acquisition and configuration requirements to ensure that wireless tactical systems are compliant with CBP and Federal Information Processing Standard (FIPS) 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 CBP select wireless tactical equipment that complies with CBP 1400-05D policies and supports the configuration requirements described in this handbook. The acquisition requirements discussed in this section include Project 25 (P25) compliance to ensure interoperability in an encrypted environment, and FIPS 140-2 compliance to ensure confidentiality.

4.1.1 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 of the standard functions and interfaces required for security functionality.

Section 4.0 of CBP 1400-05D requires that all LMR systems comply with P25 security standards. Interoperability between the wireless tactical systems of CBP, as well as those of other federal, state, and local agencies, 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.

4.1.1.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]

4.1.1.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]

[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*.

4.1.2 FIPS 140-2 Compliance

FIPS 140-2 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 140-1 and 140-2 validated cryptographic modules, along with validation certificates and security policies can be found at http://csrc.nist.gov/cryptval/140-1/1401val.htm. Each cryptographic module's security policy specifies under what modes of operation the module is FIPS validated.

4.1.2.a. All applicable wireless tactical system equipment SHALL have, at a minimum, FIPS 140-2 validated AES cryptographic modules.

4.1.2.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.

4.1.2.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 AES encryption (FIPS 197, *Advanced Encryption Standard*) 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 Service Minimization

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

4.2.2.a. All features and services that are not essential to the operation of the wireless tactical system SHALL be disabled.

4.2.3 Administrative Access Control

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

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

4.2.4 Security Auditing

Section 5.0 of CBP 1400-05D 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.

4.2.4.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
- Access to system administrator functions.

4.3 Fault Tolerance

To ensure the availability of critical systems, in particular 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. CBP 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.

4.4 Legacy Migration Requirements

Section 4.0 of CBP 1400-05D requires the migration of legacy wireless tactical systems to CBP IT security policy compliance. CBP must create migration plans for noncompliant systems outlining the provisions, procedures, and restrictions for transitioning these systems to CBP-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 140-3 compliance
- Secure peer-to-peer communication
- Secure over-the-air programming and zeroization
- 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 security policies and procedures. 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

CBP 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. CBP 1400-05D requires that appropriate awareness training SHALL be provided.

5.1.b. Any appropriate wireless security awareness training SHOULD be included in the annual training.

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

- CBP'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
  - Message 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 CBP 1400-05D, before being given access to the wireless tactical system, each employee must have specific knowledge of how to operate in a protected manner. Conventional[7] and trunked[8] radios operate differently and require different training. For example, when using a conventional system, the user must manually select a channel and assess its availability; when using a trunked system, the user must select the proper talk group.

5.2.a. Each employee's technical training SHALL include hands-on instruction on how to operate the equipment assigned to him/her within the context of his/her roles and responsibilities.

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

5.2.e. CBP SHALL include training materials as part of their accreditation package.

5.3 Future Developments

It is imperative that federal, state, and local agencies 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 CBP will support robust security mechanisms without adversely impacting the related goal of interoperability.

[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.

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

6.0.a. CBP MAY limit the applicability of the requirements listed in this document to their LMR systems only.

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

6.0.c. Within 90 days of publication of this document, CBP SHALL submit a list of their wireless tactical systems to WMO. The list SHOULD be accompanied by a statement identifying requirements that might be difficult to achieve and therefore will necessitate a waiver.

6.0.d. Within 1 year of publication of this document, CBP SHALL fully implement all its requirements.

Appendix A

References

Appendix A: Refferences

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

Department of Homeland Security, *Sensitive Systems Handbook v4.2 (DHS 4300A), September 2006*.

National Institute of Standards and Technology, *Guide for the Security Certification and Accreditation of Federal Information Systems (SP 800-37)*, May 2004.

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

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)*, November 1995.

Telecommunications Industry Association, *APCO Project 25 Trunking Overview (TSB102.AABA)*, April 1995.

Telecommunications Industry Association, *Digital Land Mobile Radio, Security Services Overview (ANSI/TIA 102.AAAB)*, August 2002.

Telecommunications Industry Association, *Project 25 Block Encryption Protocol (ANSI/TIA/EIA 102.AAAD)*, July 2002.

Telecommunications Industry Association, *Project 25 DES Encryption Protocol (ANSI/TIA/EIA 102.AAAA-A)*, February 2001.

Telecommunications Industry Association, *Project 25 Digital Radio Over-the-Air-Rekeying (OTAR) Protocol (ANSI/TIA/EIA 102.AACA)*, April 2001.

Telecommunications Industry Association, *Project 25 FDMA Common Air Interface (ANSI/TIA/EIA 102.BAAA)*, May 1998.

Telecommunications Industry Association, *Project 25 Vocoder Description (ANSI/TIA/EIA 102.BABA)*, May 1998.

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 March 2006.

Department of Homeland Security, *SAFECOM Interoperability Continuum*, http://www.safecomprogram.gov/NR/rdonlyres/5C103F66-A36E-4DD1-A00A-54C477B47AFC/0/ContinuumBrochure40505.pdf, viewed in March 2006.

National Institute of Standards and Technology, *FIPS 140-1 and FIPS 140-2 Cryptographic Modules Validation List*, http://csrc.nist.gov/cryptval/140-1/1401val.htm, viewed in March 2006.

P25 Technology Interest Group, http://www.project25.org, viewed in March 2006.

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. CBP SHALL maintain SOPs for each of the following areas: • Key management • Configuration management • Security incident response • Temporary suspension of security controls • Continuity of operations (COOP).	X	
3.0.b. CBP MAY maintain separate SOPs for different organizational elements (e.g., divisions, branches, or, in some cases, job categories), as long as every organizational element is covered by compliant SOPs.		X
3.0.c. CBP 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. CBP SHALL include minimum departmental standards in each applicable SOP.	X	
3.0.e. CBP MAY exceed a minimum departmental standard, thereby providing additional IA, 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 • Contact information for security-related questions about the SOP • Any standard CBP and 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	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 particular 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
3.1.1.d. If keys from external entities are required for interoperability purposes in the communication of SBU information, then CBP SHALL receive approval from the DHS CISO before using such keys.	X	

Mobile Feature/Configuration	Required	Recommended
3.1.1.e. If 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 • 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 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 radio devices, 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 CBP Information Systems Security Policies and Procedures Handbook 1400-05D, 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 or burned when that key is no longer required to support operations.	X	
3.1.5 Suspected Key Compromise		
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	

Mobile Feature/Configuration	Required	Recommended
3.1.5.b …This 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 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 take action 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 traffic encryption keys (TEK), which is not to exceed 90 days.	X	
3.1.6.b. KEKs that are shared across multiple radios SHALL be replaced at the same frequency as TEKs.	X	
3.1.6.b. … KEKs that uniquely identify a particular radio MAY be kept in service indefinitely.		X
3.2 Configuration Management		
3.2.a. CBP SHALL maintain documentation on the encryption configuration state of each wireless tactical system it operates.	X	
3.2.b. CBP 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

Mobile Feature/Configuration	Required	Recommended
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 • 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
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 • The date and time the work was started and finished.	X	

Mobile Feature/Configuration	Required	Recommended
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 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 radio users and other personnel to report security incidents, in accordance with CBP 1400-05D Attachment 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 • Point of contact.		X
3.3.1 Lost or Stolen Radio		
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 radio. The procedure SHALL specify that such reporting occur immediately or as soon as it is feasible to do so.	X	
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 radio. These actions SHALL include preventing the radio from authenticating to the radio network or participating in talk group.	X	
3.3.1.b …The actions SHOULD include rekeying all radios holding the same TEKs as the lost, stolen, malfunctioning, or tampered-with radio. The actions SHOULD include over-the-air zeroization of key material if this feature is available.		X

Mobile Feature/Configuration	Required	Recommended
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 • Mitigating the impact of the interference.	X	
3.3.2.b. The first technical approach to interference impact mitigation SHOULD be to change frequencies, as long as 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 back up 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 SOP SHALL specify the roles that are authorized to permit the temporary suspension of security controls. The authorized roles SHALL NOT include radio users. They MAY include an incident commander, system owner, or ISSO.	X	
3.4.b. The temporary suspension 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 radios.	X	
3.4.d. The system's Authorizing Official (AO) 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 radios in ad hoc or peer-to-peer 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	

Mobile Feature/Configuration	Required	Recommended
4.0 Technology		
4.1.1 P25 Compliance		
4.1.1.a. All procurements SHALL require that applicable wireless tactical system equipment support— P25 CAI, P25 IMBE vocoder, P25 Advanced Encryption Standard (AES) encryption.	X	
4.1.1.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
4.1.2 FIPS 140-2 Compliance		
4.1.2.a. All applicable wireless tactical system equipment SHALL have, at a minimum, FIPS 140-2 validated AES cryptographic modules.	X	
4.1.2.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
4.1.2.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 Talk Group and Channel Configuration		
4.2.1.a. Systems administrators of wireless tactical systems SHALL enable AES encryption (FIPS 197, *Advanced Encryption Standard*) 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 Service Minimization		
4.2.2.a. All features and services that are not essential to the operation of the wireless tactical system SHALL be disabled.	X	
4.2.3 Administrative Access Control		
4.2.3.a. The wireless tactical system SHALL be configured to require strong authentication in order to grant access to administrative controls.	X	
4.2.3.a. …The authentication SHOULD include a username and password.		X

Mobile Feature/Configuration	Required	Recommended
4.2.4 Security Auditing		

4.2.4.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. CBP SHALL procure, implement, and maintain a backup KMF for each wireless tactical system that uses a KMF. .	X	
4.3.a…The backup SHOULD be located at an alternate site.		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. CBP 1400-05D requires that appropriate awareness training SHALL be provided.	X	
5.1.b. Any appropriate wireless security awareness training SHOULD be included in the annual training provided at the component level.		X
5.2 Technical Training		
5.2.a. Each employee's technical training SHALL include hands-on instruction on how to operate the equipment assigned to him/her within the context of his/ her roles and responsibilities.	X	
5.2.b. CBP 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.e. CBP SHALL include training materials as part of their accreditation package	X	
6.0 USAGE		
6.0.b. Effective immediately, CBP SHALL adhere to the acquisition requirements listed in this document.	X	

Mobile Feature/Configuration	Required	Recommended
6.0.c. Within 90 days of publication of this document, CBP SHALL submit a list of their wireless tactical systems to WMO.	X	
6.0.c. …The list SHOULD be accompanied by a statement identifying requirements that might be difficult to achieve and therefore will necessitate a waiver.		X
6.0.d. Within 1 year of publication of this document, CBP SHALL fully implement all its requirements.	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
CBP	Customs and Border Protection
CCB	Change Control Board
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COOP	Continuity of Operations
CR	Change Request
DES	Data Encryption Standard
DHS	Department of Homeland Security
DoD	Department of Defense
FIPS	Federal Information Processing Standard
HF	High Frequency
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
TEK	Traffic Encryption Key
TIA	Telecommunications Industry Association
VHF	Very High Frequency
WMO	Wireless Management Office
WSB	Wireless Security Board