U.S. Customs and Border Protection

Attachment Q4

Sensitive RFID 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 radio frequency identification (RFID) 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 4.6, Wireless Communications. Within Attachment Q4, the use of the word "shall" shall be considered mandatory only in as it applies to existing CBP policy elements. Attachment Q4 also includes concepts and practices from other federal entities with established wireless security programs, such as the National Institute of Standards and Technology (NIST) and Department of Defense (DoD).

1.1 Purpose

This document defines the CBP wireless security policy beyond CBP 1400-05D as it pertains to RFID. The handbook provides a minimum set of management, operational, and technical controls that CBP is required to implement and monitor compliance. It also suggests best practices and options that CBP should consider when managing its RFID systems.

1.2 Scope

This document addresses the security elements of RFID systems which utilize passive tags. Although RFID systems might involve various technologies and applications, this handbook is targeted specifically at asset management systems that CBP would implement.

1.3 Authority

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

1.4 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 RFID systems security.
- Section 3 (Standard Operating Procedures) describes how components should document their operational practices to support RFID systems security.
- Section 4 (Technology) focuses on the features that must be considered when acquiring and configuring RFID systems.
- Section 5 (Training and Exercises) reviews methods for ensuring that staff are aware of security threats and requirements and can use their RFID systems in a secure manner.

1.5 Revisions to the Handbook

The Wireless Management Office (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 may 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 updates on RFID technology because the technology is rather new and constantly changing.

2.0 GOVERNANCE

Effective 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 CISO, formulates and coordinates department-wide policies and guidelines related to the security of wireless services and technologies, including RFID 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 information technology programs and system development initiatives. In addition, the WSB is used as a forum for identifying and resolving emerging wireless security issues and concerns.

This handbook represents the WMO's primary mechanism for providing policy and guidance with respect to radio frequency identification systems.

2.2 RFID Usage Policy

The RFID usage policy describes how the implemented RFID system should be used. It is meant to be used if CBP is using or considering implementing RFID technologies. This policy describes the authorized and unauthorized uses of RFID technologies related to particular RFID system tasks. The policy should be consistent or integrated with CBP's privacy and security policy.

2.2.a. CBP SHALL specifically document and ensure that the use and users of RFID comply with this and all other related CBP RFID security and privacy policies.

2.3 Agreements With External Organizations

RFID systems sharing data across agency boundaries will require formal agreements such as memoranda of agreement (MOA), memoranda of understanding (MOU), or interconnection security agreements (ISA) between the two or more components. These agreements specify the network connections and authentication mechanisms to be used by the components involved. These agreements reduce the potential for subsequent misunderstandings and potential security breaches.

2.3.a. CBP SHALL institute an MOA, MOU, or ISA if sharing RFID information with an external organization. External organizations may include but are not limited to other government departments (e.g., DoD, Department of Energy [DOE], Department of State [DOS]), private individuals, corporations, and non-governmental organizations (e.g., Red Cross).

2.3.b. A third party SHALL audit compliance with the external organization's agreement.

2.4 Privacy

All uses of technology within the CBP must comply with privacy protection requirements. The identification and analysis of potential privacy risks and issues should begin as soon as the program office defines the system and use of technology. Identifying potential privacy issues early in the process makes the incorporation of privacy protection design and operational requirements easier, faster, and more cost effective.

There are two existing mechanisms within the CBP to ensure that technologies (i.e., RFID technologies) sustain privacy protections.

The first mechanism, Privacy Compliance, uses standardized privacy compliance documentation to identify and respond to privacy issues within specific systems and programs. Three documents are in increasing levels of complexity and severity:

- **Privacy Threshold Analysis (PTA)—**is a short click-through form that focuses on whether the system or program uses personally identifiable information. The program office completes this form and submitted it to the DHS Privacy Office for review. The review of the PTA determines the requirement to complete the second form, the Privacy Impact Assessment (PIA).
- **PIA—**is a longer form that requires thorough answers to a series of detailed questions focused on identifying and analyzing the detailed privacy issues that raised by the system/program. The results of the PIA trigger the possible requirement to create or amend a System of Records Notice (SORN).
- **SORN—**describes the categories of users and uses of a collection of information records and grants legal rights to individuals who are the subject of the collection of records.

The second mechanism, Privacy Technology Policy (PTT), identifies those overall policy issues and vehicles for integrating privacy protections into the overall management of a particular technology. This mechanism, which is less standardized in form, is focused on raising general awareness and integration of privacy protection such that future uses of technology benefit from the privacy assessments of previous uses. This approach seeks administrative and organizational

vehicles, like the present document, to integrate the relevant privacy protection requirements into existing Department and CBP processes that apply to the use of a technology.

To properly ensure that privacy risks are identified and the issues are addressed, program offices that are contemplating using RFID technology should initiate the privacy compliance mechanism and coordinate with the DHS Privacy Office for specific privacy technology guidance related to RFID.

To begin the privacy compliance process, the program office should obtain a copy of the Privacy Threshold Analysis template from the DHS Privacy Office or through its website (www.dhs.gov/privacy and on DHSOnline), answer the questions, and return the completed form to the DHS Privacy Office (pia@dhs.gov, (b)(6) (b)(7)(C)).

To begin the privacy technology policy process, the program office should contact the Director of Privacy Technology within the DHS Privacy Office (privacy@dhs.gov, (b)(6) (b)(7)(C)).

As a procedural matter, the DHS Privacy Office will coordinate the privacy compliance and privacy technology efforts to ensure that the program benefits from both perspectives in unity. As a preparatory matter, the program office should initiate both mechanisms as early in the program's development process as possible because both mechanisms could substantially affect the design, operation, and administration of the RFID system or technology.

The DHS *Certification and Accreditation (C&A) Guidance for Sensitive but Unclassified (SBU) Systems: Users Manual* provides additional detailed information about PTA and PIA processes. Refer to the CBP Information Systems Security Policies and Procedures Handbook, 1400-05D, Privacy Impact Assessment section, for additional information.

2.4.a. CBP SHALL perform a PTA for each use of RFID technology and identify whether the project could relate in any way to an individual (please reference question 4 of the PTA).

2.4.b. CBP SHALL perform a PIA if tags store or associate with personally identifiable information.

2.4.c. The use of the tags and all associated data should be limited to the intended area of operation and SHOULD NOT be used in any way connected with the individual outside that area of operation. This limitation should be specifically addressed in the associated privacy compliance documentation and audit table.

2.4.d. CBP and third parties SHOULD NOT be able to determine an individual's location based on the location of the tag outside the tag's intended area of operation.

2.4.e. CBP and third parties SHOULD NOT be able to reveal specific information based on a specific tag outside of the tag's intended area of operation.

2.5 Future Developments

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

- Sharing of governance best practices across CBP to improve internal governance of RFID systems.
- Development of governance structures involving organizations outside CBP to support interoperability of communication between CBP and these external entities.

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. SOPs SHALL be maintained for each of the following areas:

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

3.0.b. Separate SOPs MAY be maintaind for different organizational elements (e.g., divisions, branches, or occasionally job categories), as long as every organizational element is covered by compliant SOPs.

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

3.0.d. The SOPs SHALL be incorporated into the privacy compliance documentation and both the SOP and the privacy compliance documentation SHALL be maintained in alignment as one or both change over time.

The remainder of this section explains the content of each SOP in more detail. CBP is provided the discretion to write SOPs in a manner appropriate to their mission and operational environment; in most cases, the SOP requirements listed in the 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.e. A CBP MAY exceed a minimum departmental standard, thereby providing additional information assurance, 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 DHS or CBP notices or warnings.

3.1 Physical Access Control

General physical access controls restrict the entry and exit of personnel from an area, such as an office building, data center, or room containing IT equipment. These controls protect against threats associated with the physical environment. It is important to review the effectiveness of general physical access controls in each area during business hours and at other times. Effectiveness depends not only on the characteristics of the controls used but also on their implementation and operation.

RFID signals may travel outside the walls and perimeter of where the system is being used. RFID system owners need to use physical access controls to limit the ability of an adversary getting close enough to RFID system physical components to compromise RFID data security.

In addition to concerns regarding specific adversaries, consideration should be given to ensuring that the use of the data related to the RFID system is only and always used appropriately. This action includes preventing all unintended and/or inappropriate use even by populations that are not strictly considered adversarial. As mentioned above, the potential misuse (including unintended use) of RFID system/data must be identified in the privacy compliance documentation and that documentation must be kept updated as new uses and new risks are identified.

Refer to the CBP Information Systems Security Policies And Procedures handbook, 1400-05D, General Physical Access section, for additional physical access security policy.

3.1.a. CBP SHALL include a combination of physical access controls that could include fences, gates, walls, locked doors, turnstiles, surveillance cameras, tamper-resistant packaging, and security guards.

3.1.b. CBP SHALL perform a perimeter test to measure the effective range of RFID signals to test the ability for adversaries to capture RFID system data that could potentially leak outside the RFID system perimeter boundaries.

3.1.c. CBP SHOULD use RF shielding on the perimeter of the RFID system implementation.

3.2 Appropriate Placement of RFID Equipment

RFID systems emanate RF signals that have the potential to cause harm to certain materials and chemicals if exposed over time. RFID system equipment can be strategically placed to reduce unnecessary electromagnetic radiation.

3.2.a. CBP SHALL assess hazards of electromagnetic radiation (hazards of electromagnetic radiation to ordnance [HERO]/hazards of electromagnetic radiation to fuel [HERF]/hazards of electromagnetic radiation to people [HERP]). Please reference:

- Federal Communications Commission (FCC), Office of Engineering and Technology (OET). OET Bulletin 56, Fourth Edition, August 1999
- DoD Directive 3222.2 “DoD Electromagnetic Environmental Effects (E3) Program”
- FCC 47 *Code of Federal Regulations* (CFR) §§ 1.1307(b), 1.1310, 2.1091, and 2.1093.
- Radio Frequency Safety—Office of Engineering and Technology: http://www.fcc.gov/oet/rfsafety/

3.2.b. If HERO/HERF/HERP assessments determine that risks exist, CBP SHALL establish minimum safe distances, maximum power levels, or duty cycles.

3.3 Secure Disposal of Tags

RFID tags should be securely disposed of after they have performed their intended task. Tags can be physically or electronically destroyed or deactivated. Physical destruction involves

incineration, manual tearing, or shredding. Shredding and tearing will result in separating the integrated circuit from the antenna (which makes the tag considerably more difficult to read but not impossible) or will damage or obliterate the integrated circuit. Therefore, incineration may be required if zero readability post-physical destruction is mandated. Electronic destruction involves using either a tag's kill feature or a very strong electromagnetic field to send a high current through the RFID circuit to render the tag's circuitry inoperable. Permanently disabling tags eliminates the possibility of tag reuse that could lead to numerous problems and can also sustain privacy protections. (b)(7)(E) (b)(7)(E) incineration might be required if zero readability post-physical destruction is mandated. Refer to the CBP Information Systems Security Policies And Procedures Handbook, 1400-05D, Media Sanitization and Disposal section, for additional policy.

3.3.a. Tags SHOULD be securely disposed of by physical or electrical means after they have performed their intended task. If the tag is used in connection with individuals, the tag SHALL be securely disposed of after intended task is completed.

3.4 Separation of Duties

Separation of duties (required by OMB Circular No. A-130) mandates the assignment of portions of security-related tasks to several individuals. This separation is required for adequate internal control of sensitive IT systems. This also ensures that no single individual has total control of the system's security mechanisms and prevents a single individual acting alone from subverting a critical process or otherwise completely compromising the system.

The separation of duties of RFID system administrators ensures that duties are assigned to more than one individual in a manner so that no one person can control the RFID tagging and reading process from start to finish. Refer to the CBP Information Systems Security Policies And Procedures Handbook, 1400-05D, Separation of Duties section 4.1.4, for additional policy.

3.4.a. CBP SHOULD separate the role of tagging and reading tags to more than one individual at each RFID system implementation when tagged items are of high value or contain sensitive user/component information.

3.5 Configuration Management

Configuration management controls changes to RFID systems to ensure that these changes are consistent with the organization's mission. 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.

Refer to the CBP Information Systems Security Policies And Procedures Handbook, 1400-05D, Configuration Management section 3.7, for additional policy.

3.5.a. The configuration management SOP SHALL specify the membership of the Configurations Control Board (CCB). The CCB membership SHOULD be based on personnel roles rather than named individuals.

3.5.b. 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:

- Purpose of the change
- Specific equipment or systems that the change will affect
- Date and time the change will be performed
- Duration of work
- Whether the change is expected to cause a temporary outage or performance degradation
- Personnel who will be performing the change
- Rollback procedure in case the change does not have its intended effect.

3.5.c. The configuration management SOP SHALL specify the voting procedure for CR approval. Approval SHOULD require unanimous written consent by 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.

3.5.d. The configuration management SOP SHALL specify an emergency change procedure for any configuration changes that needs to occur before a meeting of the CCB to restore the availability or security of the system.

3.5.e. 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 later than 48 hours after the change. The configuration management SOP SHOULD require that the system be rolled back to its state before the emergency whenever an emergency CR is not approved.

3.5.f. The configuration management SOP SHOULD include controls related to the appropriate separation of duties. Individuals who load tags SHOULD NOT be permitted to read the tags.

3.5.g. 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 needed to be added or removed to achieve the desired result
- The date and time the work was started and finished.

3.5.h. Retirement or disposal of system hardware SHALL be considered a configuration change. The configuration management SOP SHALL specify the procedure for sanitizing RFID system components of key material and other sensitive data before disposal. The authorized techniques SHALL NOT include simple file deletion or tag disposal. They SHALL include zeroization or degaussing for RFID system components, and destruction or using a KILL command for RFID tags.

3.5.i. The configuration management SOP SHALL specify the recordkeeping requirements of CCB proceedings. Approved CRs and approved ARs SHALL be maintained for a period not less than 1 year. They SHOULD be maintained for the operational lifetime of the system.

3.6 Security Incident Response

Most security controls are designed to protect an organization against security threats but 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.

3.6.a. The Security Incident Response SOP SHALL specify methods for RFID system users and other personnel to report security incidents, in accordance with CBP 1400-05D, Attachment F and NIST Special Publication 800-61, "Computer Security Incident Handling Guide." If the tag is used in connection with individuals, Security Incident Response SOP SHALL include a requirement to also report incidents to the DHS and CBP Privacy Office.

3.6.1 Radio Frequency Interference

Radio interference can cause transmitted signals to not be properly received. Determining the potential sources of radio interference for a particular RFID implementation requires a site survey. Nearly all RFID systems operate in nonlicensed frequency bands (range). They may experience radio interference from other systems that share the same frequency band. For example, wireless networking equipment, cordless telephones, and other wireless consumer devices use the microwave 2.4 and 5.8 gigahertz bands, so they represent a potential source of interference for RFID systems that use these frequencies.

3.6.1.a. A site survey SHOULD be conducted before the deployment of an RFID subsystem to check for radio interference with the planned system.

3.6.1.b. The security incident response SOP SHALL specify actions to take after radio users detect radio interference. The actions SHALL at a minimum include the following:

- Notifying a relevant authority that the interference is occurring
- Mitigating the impact of the interference such as by the implementation of shielding.

3.6.1.c. If radio interference cannot be circumvented, personnel SHOULD switch to a backup form of tracking assets such as barcodes or paper-based systems if the interference is degrading mission performance.

3.6.1.d. The security incident response SOP MAY cover procedures for identifying 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.

3.6.1.e. CBP SHALL receive radio frequency (RF) authorization from the National Telecommunications and Information Administration (NTIA) Office of Spectrum Management (OSM), http://www.ntia.doc.gov/osmhome/osmhome.html.

3.7 Continuity of Operations Planning

The COOP planning element of this program requires CBP to develop, test, exercise, and maintain comprehensive plans so that essential CBP business functions can be continued following an emergency situation. Business-oriented COOP plans focus on sustaining an organization's essential functions at an alternate site until the primary site can be restored.

Refer to the CBP Information Systems Security Policies And Procedures Handbook, 1400-05D, Continuity of Operations Planning section, for additional policy.

3.7.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.

3.7.b. The COOP SOP SHALL list other authorized mechanisms for tracking assets when the RFID system is unavailable. Such mechanisms MAY include the use of barcodes or paper-based tracking.

3.7.c. The COOP SOP SHALL specify the circumstances under which personnel should operate backup tracking methods (e.g., when infrastructure connectivity is unavailable).

3.8 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 between CBP, other components or federal agencies, or between CBP and state and local organizations supporting RFID logistics operations.
- Additional guidance related to the certification process for RFID systems that addresses specific technologies and protection mechanisms.
- SOPs to support the creation, use, and breakdown of ad hoc or peer-to-peer networks when centralized infrastructure is unavailable or for whatever 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.
- All changes to SOP SHALL be reflected in the relevant portions of all privacy compliance documentation and any privacy protection requirements that are triggered by the changes SHALL be incorporated into the SOPs before the implementation of the new SOPs.

4.0 TECHNOLOGY

Properly configured technology is a critical component of IA. This section covers acquisition and configuration requirements to ensure that RFID systems are compliant with CBP requirements and that it supports the SOPs discussed in Section 3.0.

4.1 Technical Security Controls

Technical security controls focus on security controls that a computer system executes. These controls provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

Some technical controls available to RFID systems include controlling the RF interface to tags, password protection, and LOCK and KILL commands that can be sent to block or disable tags. A password would be required before the tag would accept the LOCK or KILL command.

4.1.1 Authentication

Authentication is the process of proving that a subject is who the subject claims to be. Authentication is a measure used for verifying the eligibility of a subject and the ability of that subject to access certain information. Some tags have on-board security features that allow the protection of sensitive information stored in the tag.

Refer to the CBP Information Systems Security Policies And Procedures Handbook, 1400-05D, Identification and Authentication section 5.1, for additional policy.

4.1.1.a. Readers SHALL have strong, unique administrative passwords to support user authentication.

4.1.2 Tag Data Protection

The access password may be used to restrict access to a tag or to parts of a tag's memory, where applicable. A reader must transmit the correct access password to the tag to access restricted data on the tag.

4.1.3 Minimizing Data Stored on Tags

RFID tags can hold more information than legacy technology such as barcodes. RFID system owners must be aware of the data and the sensitivity of the data stored in the transponders. In most applications, the RFID transponder can be given a unique identifier number that can be linked with additional information at a secure, controlled centralized database. (b)(7)(E)

(b)(7)(E)

4.1.3.a. CBP SHOULD NOT use tags to hold more than a unique identifier unless approved by the Authorizing Official (AO).

4.1.3.b. Consideration SHOULD be given to using nonstatic identifiers in tags to minimize the ability of one card (identifier) being recorded (identified and potentially tracked) across places and time. Reducing the potential for this sort of tracking supports privacy and security protections.

4.2 Configuration Requirements

Even if a system meets all acquisition requirements, it must be properly configured to comply with CBP security policy. This section addresses tag and reader configuration, service minimization, administrative access control, and security auditing.

4.2.1 Security Auditing

Section 5.0 of CBP 1400-05D requires that audit trails be sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. The ability to audit a system user's actions, along with the use of individually assigned authentication controls, provides accountability. Audit records provide security managers with a way to detect misuse or intrusion, identify exposed sensitive data, and occasionally track the source of the security breach.

The uses of audit records also support privacy protections by verifying that all actual uses are previously known and that only identified and appropriate uses are occurring—in fact, no inappropriate uses are occurring.

4.2.1.a. The RFID 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:

- Deactivation of a security feature
- Successful and unsuccessful logins
- Access to system administrator functions.

4.2.1.b. The auditing process SHALL be described as part of the privacy compliance analysis and documentation process to ensure that that data is only and always used appropriately.

4.3 Fault Tolerance

To ensure the availability of critical systems, in particular those supporting security functionality, organizations build redundancies through their RFID systems so that if a system component fails, a backup exists to continue operations. Some of these backups may include relying on barcodes or deploying a paper-based system.

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 or her actions and is educated regarding the component's security policies and procedures. Security training includes security awareness and technical training courses. Operational exercises reinforce the lessons learned and present employees with an opportunity to put their training into practice.

5.1 Security Awareness Training

CBP cannot ensure the security of its RFID system without the knowledge and active participation of its employees in the implementation of sound security principles.

5.1.a. CBP is reminded that 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 RFID systems, an employee SHOULD, at a minimum, have knowledge of the following:

- The CBP's security policy and SOPs related to the RFID system
- RFID Usage Policy
- Network SOPs
- How to identify, respond to, and report security incidents, including the following:
  - Lost or stolen tag
  - Radio frequency interference
  - Broken or tampered-with tag.

5.2 Technical Training

In addition to the security awareness training required by CBP 1400-05D, before being given access to an RFID system, each employee must have specific knowledge of how to operate in a secure manner that will not compromise the RFID system and that will sustain privacy protections.

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

5.2.b. CBP SHALL ensure that newly hired employees have obtained initial technical training before giving them access to the RFID system.

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

5.2.d. Security and privacy technical training MAY be combined with other technical training related to the RFID system.

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

Appendix A

References

APPENDIX A: REFERENCES

DHS WMO Wireless Applications Implementation Guide for RFID, March 2006.

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, *Guidance for Securing Radio Frequency Identification Systems (Draft) (SP 800-98)*, September 2006.

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.

Appendix B

Checklist for Securing RFID Systems

APPENDIX B: CHECKLIST FOR SECURING RFID SYSTEMS

Mobile Feature/Configuration	Required	Recommended
Security Requirements for All RFID Systems		
2.2 RFID Usage Policy		
2.2.a. CBP SHALL specifically document and ensure that the use and users of RFID comply with this and all other related DHS and CBP RFID security and privacy policies.	X	
2.3 Agreements With External Organizations		
2.3.a. CBP SHALL institute an MOA, MOU, or ISA if sharing RFID information with an external organization. External organizations may include but are not limited to other government departments (e.g., DoD, Department of Energy [DOE], Department of State [DOS]), private individuals, corporations, and non-governmental organizations (e.g., Red Cross).	X	
2.3.b. A third party SHALL audit compliance with the external organization's agreement.		X
2.4 Privacy		
2.4.a. CBP SHALL perform a PTA for each use of RFID technology and identify whether the project could relate in any way to an individual (please reference question 4 of the PTA).	X	
2.4.b. CBP SHALL perform a PIA if tags store or associate with personally identifiable information.	X	
2.4.c. The use of the tags and all associated data should be limited to the intended area of operation and SHOULD NOT be used in any way connected with the individual outside that area of operation. This limitation should be specifically addressed in the associated privacy compliance documentation and audit table.		X
2.4.d. CBP and third parties SHOULD NOT be able to determine an individual's location based on the location of the tag outside the tag's intended area of operation.		X
2.4.e. CBP and third parties SHOULD NOT be able to reveal specific information based on a specific tag outside the tag's intended area of operation.		X
3.0 Standard Operating Procedures		
3.0.a. CBP SHALL maintain SOPs for each of the following areas: • 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 occasionally 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 may review the SOPs' security procedures and requirements for compliance with CBP 1400-05D	X	

3.0.d. The SOPs SHALL be incorporated into the privacy compliance documentation and both the SOP and the privacy compliance documentation SHALL be maintained in alignment as one or both change over time.	X	
3.0.e. CBP MAY exceed a minimum departmental standard, thereby providing additional information assurance, 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 DHS or CBP notices or warnings.	X	
3.1 Physical Access Control		
3.1.a. CBP SHALL include a combination of physical access controls that could include fences, gates, walls, locked doors, turnstiles, surveillance cameras, tamper-resistant packaging, and security guards.	X	
3.1.b. CBP SHALL perform a perimeter test to measure the effective range of RFID signals to test the ability for adversaries to capture RFID system data that could potentially leak outside the RFID system perimeter boundaries.	X	
3.1.c. CBP SHOULD use RF shielding on the perimeter of the RFID system implementation.		X
3.2 Appropriate Placement of RFID Equipment		
3.2.a. CBP SHALL assess hazards of electromagnetic radiation (hazards of electromagnetic radiation to ordnance [HERO]/hazards of electromagnetic radiation to fuel [HERF]/hazards of electromagnetic radiation to people [HERP]HERO/HERF/HERP). Please reference: • Federal Communications Commission (FCC), Office of Engineering and Technology (OET). OET Bulletin 56, Fourth Edition, August 1999 • DoD Directive 3222.2 "DoD Electromagnetic Environmental Effects (E3) Program" • FCC 47 *Code of Federal Regulations* (CFR) §§ 1.1307(b), 1.1310, 2.1091, and 2.1093 • Radio Frequency Safety—Office of Engineering and Technology: http://www.fcc.gov/oet/rfsafety/	X	
3.2.b. If HERO/HERF/HERP assessments determine that risks exist, components SHALL establish minimum safe distances, maximum power levels, or duty cycles.	X	
3.3 Secure Disposal of Tags		
3.3.a. Tags SHOULD be securely disposed of through physical or electrical means after they have performed their intended task.		X
3.3.a. … If the tag is used in connection with individuals, the tag SHALL be securely disposed of after intended task is completed.	X	
3.4 Separation of Duties		
3.4.a. CBP SHOULD separate the role of tagging and reading tags to more than one individual at each RFID system implementation when tagged items are of high value or contain sensitive user/component information.		X

3.5 Configuration Management		
3.5.a. The configuration management SOP SHALL specify the membership of the Configurations Control Board (CCB).	X	
3.5.a. …The CCB membership SHOULD be based on personnel roles rather than named individuals.		X
3.5.b. 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: • Purpose of the change • Specific equipment or systems that the change will impact • Date and time the change will be performed • Duration of the work • Whether the change is expected to cause a temporary outage or performance degradation • Personnel who will be performing the change • Rollback procedure in case the change does not have its intended effect.	X	
3.5.c. The configuration management SOP SHALL specify the voting procedure for CR approval.	X	
3.5.c. … Approval SHOULD require unanimous written consent by 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
3.5.d. The configuration management SOP SHALL specify an emergency change procedure for any configuration changes that needs to occur before a meeting of the CCB to restore the availability or security of the system.	X	
3.5.e. The configuration management SOP SHALL require timely submission of an emergency CR for retroactive approval of each emergency change.	X	
3.5.e. …The time frame for submission of an emergency CR SHOULD be no later than 48 hours after the change. The configuration management SOP SHOULD require that the system be rolled back to its state before the emergency whenever an emergency CR is not approved.		X
3.5 f. The configuration management SOP SHOULD include controls related to the appropriate separation of duties. Individuals who load tags SHOULD NOT be permitted to read the tags.		X
3.5.g. 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 needed to be added or removed to achieve the desired result • The date and time the work was started and finished.	X	

3.5 h. Retirement or disposal of system hardware SHALL be considered a configuration change. The configuration management SOP SHALL specify the procedure for sanitizing RFID system components of key material and other sensitive data prior to disposal. The authorized techniques SHALL NOT include simple file deletion or tag disposal. They SHALL include zeroization or degaussing for RFID system components, and destruction or using a KILL command for RFID tags.	X	
3.5.i. The configuration management SOP SHALL specify the recordkeeping requirements of CCB proceedings. Approved CRs and approved ARs SHALL be maintained for a period not less than 1 year. They SHOULD be maintained for the operational lifetime of the system.	X	
3.6 Security Incident Response		
3.6.a. The Security Incident Response SOP SHALL specify methods for RFID system users and other personnel to report security incidents, in accordance with CBP 1400-05D, Attachment F and NIST Special Publication 800-61, "Computer Security Incident Handling Guide." If the tag is used in connection with individuals, Security Incident Response SOP SHALL include a requirement to also report incidents to the DHS and CBP Privacy Office.	X	
3.6.1 Radio Frequency Interference		
3.6.1.a. A site survey SHOULD be conducted before the deployment of an RFID sub-system to check for radio interference with the planned system.		X
3.6.1.b. The security incident response SOP SHALL specify the actions to take after radio users detect radio interference. The actions SHALL at a minimum include the following: • Notifying a relevant authority that the interference is occurring • Mitigating the impact of the interference such as by the implementation of shielding	X	
3.6.1.c. If radio interference cannot be circumvented, personnel SHOULD switch to a backup form of tracking assets such as barcodes or paper-based systems if the interference is degrading mission performance.		X
3.6.1.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
3.6.1.e. CBP SHALL receive radio frequency (RF) authorization from the National Telecommunications and Information Administration (NTIA) Office of Spectrum Management (OSM), http://www ntia.doc.gov/osmhome/osmhome.html.	X	
3.7 Continuity of Operations Planning		
3.7.a. The COOP SOP SHALL specify the roles and responsibilities of personnel during a significant system outage.	X	
3.7.a. …A personnel notification roster SHOULD be distributed among all relevant personnel for use during emergencies or significant outages.		X
3.7.b. The COOP SOP SHALL list other authorized mechanisms for tracking assets when the RFID system is unavailable. Such mechanisms MAY include the use of barcodes or paper-based tracking.	X	
3.7.c. The COOP SOP SHALL specify the circumstances under which personnel should operate backup tracking methods (e.g., when infrastructure connectivity is unavailable).	X	
4.0 Technology		
4.1.1 Authentication		

4.1.1.a. Readers SHALL have strong, unique administrative passwords to support user authentication.	X	
4.1.3 Minimizing Data Stored on Tags		
4.1.3.a. CBP SHOULD NOT use tags to hold more than a unique identifier unless approved by the Authorizing Official (AO).		X
4.1.3.b. Consideration SHOULD be given to using nonstatic identifiers in tags to minimize the ability of one card (identifier) being recorded (identified and potentially tracked) across places and time. Reducing the potential for this sort of tracking supports privacy and security protections.		X
4.2.1 Security Auditing		
4.2.1.a. The RFID 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: • Deactivation of a security feature • Successful and unsuccessful logins • Access to system administrator functions.	X	
4.2.1.b. The auditing process SHALL be described as part of the privacy compliance analysis and documentation process to ensure that that data is only and always used appropriately.	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
5.1.c. Upon completion of the security awareness training for RFID systems, an employee SHOULD, at a minimum, have knowledge of the following: • The CBP's security policy and SOPs related to the RFID system • RFID Usage Policy • Network SOPs • How to identify, respond to, and report security incidents, including the following: ○ Lost or stolen tag ○ Radio frequency interference ○ Broken or tampered-with tag.		X
5.2 Technical Training		
5.2.a. Each employee's technical training SHALL include hands-on instruction on how to operate the RFID equipment assigned to him/her within the context of his or her roles and responsibilities.	X	
5.2.b. CBP SHALL ensure that newly hired employees have obtained initial technical training before giving them access to the RFID system.	X	
5.2.c. Technical training courses for system users and system administrators SHALL include security- and privacy-related instructions.	X	

5.2.d. Security and privacy technical training MAY be combined with other technical training related to the RFID system.		X
5.2.e. CBP SHALL include training materials as part of their accreditation package.	X	

Appendix C

Physical and Environmental Security

APPENDIX C: PHYSICAL AND ENVIRONMENTAL SECURITY

The following controls SHOULD be considered to protect RFID system infrastructure from physical and environmental threats:

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

Appendix D
Acronyms

APPENDIX D: ACRONYMS

AO	Authorizing Official
AR	After-action Report
C&A	Certification and Accreditation
CBP	Customs and Border Protection
CCB	Change Control Board
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COOP	Continuity of Operations
CR	Change Request
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOS	Department of State
E3	Electromagnetic Environmental Effects
FCC	Federal Communications Commission
HERF	Hazards of Electromagnetic Radiation to Fuel
HERO	Hazards of Electromagnetic Radiation to Ordnance
HERP	Hazards of Electromagnetic Radiation to People
IA	Information Assurance
ISA	Interconnection Security Agreement
IT	Information Technology
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
OET	Office of Engineering and Technology
OPSEC	Operations Security
OSM	Office of Spectrum Management
PIA	Privacy Impact Assessment

PTA	Privacy Threshold Analysis
PTT	Privacy technology Policy
RF	Radio Frequency
RFID	Radio Frequency Identification
SOP	Standard Operating Procedure
SORN	System of Records Notice
SP	Special Publication
WMO	Wireless Management Office
WSB	Wireless Security Board