Homeland Security

DHS 4300A
Sensitive Systems Handbook

Attachment Q4

Sensitive RFID Systems

Version 11.0

August 5, 2014

Protecting the Information that Secures the Homeland

DOCUMENT CHANGE HISTORY

Version	Date	Description
0.1	November 2nd, 2006	Initial release
0.1	December 7, 2006	Adjudicated comments from Adjudication Table 0.1
0.2	January 22, 2007	Accepted comments from Adjudication Table 0.1 (RFID WG feedback)
5.0	March 1, 2007	No change
6.0	May 14, 2008	No change
6.1	September 23, 2008	No change
7.0	August, 2009	Introduced new terminology Authorizing Official (AO) – replaces DAA, as per NIST 800-37 and 800-53
11.0	August 5, 2014	Thorough rewrite. Major change to reflect new RFID technology development.

CONTENTS

1.0 INTRODUCTION

This document provides requirements and guidance to assist Department of Homeland Security (DHS) Components in development and implementation of Information Assurance (IA) programs for their Radio Frequency Identification (RFID) systems. It is a supplement to the DHS 4300A Sensitive Systems Handbook and is intended to be read in conjunction with that document, especially Section 4.6 Wireless Network Communications. In this document, statements using the word "shall" are mandatory only when DHS policy elements apply. Attachment Q4 also incorporates RFID security policies and guidelines from other entities such as the National Institute of Standards and Technology (NIST), Department of Defense (DoD), and national and international standardization organizations. General security best practices commonly recommended and followed by private industry and academic communities are also included.

1.1 Purpose

This document provides guidance for implementation the DHS wireless security policy beyond DHS 4300A as it pertains to RFID. The handbook provides a minimum set of management, operational, and technical controls that DHS Components are required to implement and with which they are expected to monitor compliance. It also suggests best practices and options that DHS Components should consider when managing RFID systems.

Future revisions of this document are expected to include updates on RFID technology, which is relatively new and constantly changing.

1.2 Scope

This document addresses the security elements of RFID systems which use passive or active RFID technologies. Although RFID systems may involve various technologies and applications, this Handbook Attachment is targeted mainly at asset management systems that DHS would implement.

1.3 Authority

This document is issued as user guidance by authority of the DHS Chief Information Officer (CIO) through the Office of the Chief Information Security Officer (CISO).

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.

In accordance with DHS Sensitive Systems Policy Directive 4300A, AOs must approve the technology, application, implementation, and use of RFID systems at a specified risk level during the security authorization process and ensure that appropriate and effective security measures are included in security plans.

AOs should pay particular attention to the risks that must be considered in approving RFID systems that have technological barriers to adoption of the system security plan's provisions.

AOs should ensure that they understand the risks associated with a particular RFID system, and that risks are measured and mitigated to an acceptable level.

2.1 RFID Usage Policy

The RFID usage policy describes how the RFID system that is implemented should be used. The usage policy is intended to be used by all DHS Components that use or are considering implementing RFID technologies. The usage policy describes the authorized and unauthorized uses of RFID technologies related to particular RFID system tasks. The policy should be consistent or integrated with each DHS Component's privacy and security policy.

2.2 Agreements with External Organizations

DHS Components that implement 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 Privacy

All uses of technology within the Department 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.

2.4 Future Governance 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 DHS so that Components can improve their internal governance of RFID systems

3.0 DEVELOPMENT OF INTEROPERABILITY GOVERNANCE STRUCTURES

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.

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

3.1 Physical Access Control

General physical access controls restrict the entry and exit of personnel from areas such as office buildings, data centers, and rooms 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 can travel outside the walls and perimeter of the area in which the system is being used; therefore, RFID system owners need to use physical access controls to limit the ability of an adversary to get close enough to RFID system physical components to compromise 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 always used only appropriately. This means preventing unintended or inappropriate use even by personnel not strictly considered adversaries. Potential misuse (including unintended use) of RFID systems and data must be covered in privacy compliance documentation, and that documentation which must be kept updated as new uses and new risks are identified.

Refer to the General Physical Access section of DHS Sensitive Systems Policy Directive 4300A for additional physical access security policy.

3.2 Appropriate Placement of RFID Equipment

RFID systems propagate radio frequency (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.

3.3 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; permanently disabling also sustains privacy protection. Although often impractical, it might still be possible to retrieve the tag contents from a disabled tag (e.g., by employing a scanning electron microscope); therefore, incineration might be required if zero readability post-physical destruction is mandated. Refer to the *DHS 4300A Sensitive Systems Handbook*, Media Sanitization and Disposal section, for additional guidance.

3.4 Separation of Duties

Office of Management and Budget (OMB) Circular No. A-130 mandates separation by assignment of each security task to several individuals, with no single individual responsible for

an entire task. Separation in this manner is required for adequate internal control of sensitive IT systems. It also ensures that no single individual has total control of the system's security mechanisms.

The separation of duties of RFID system administrators ensures that duties are assigned to more than one individual in such a manner that no one person can control the RFID tagging and reading process from start to finish. Refer to the DHS 4300A Sensitive Systems Handbook, Separation of Duties section, for additional guidance.

3.5 Configuration Management

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

Refer to the DHS 4300A Sensitive Systems Handbook, Configuration Management section, for additional guidance.

3.6 Security Incident Response

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.

3.6.1 Radio Frequency Interference

One system's propagation of RF can interfere with the clarity of another system's traffic.. Determining potential sources of radio interference for a particular RFID implementation requires a site survey. Nearly all RFID systems operate in non-licensed frequency bands, and 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 all use the 2.4 and 5.8 gigahertz frequency bands, so they represent a potential source of interference for RFID systems that use these frequencies.

RF use authorization, if required, is obtained 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 DHS Components to develop, test, exercise, and maintain comprehensive plans so that essential DHS 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 DHS 4300A Sensitive Systems Handbook, Continuity of Operations Planning section, for additional guidance.

3.8 Security Auditing

Section 5.3 of DHS Sensitive Systems Policy Directive 4300A 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 trail records provide security managers with a means of detecting misuse or intrusion, identifying exposed sensitive data, and can enable tracking the source of the security breach.

The uses of audit trail 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, that no inappropriate uses are occurring.

3.9 Future Developments

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

- SOPs to support interoperability across multiple Components or Federal agencies, or between DHS Components 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 *DHS 4300A Sensitive Systems Handbook*, Attachment G ("Rules of Behavior"
- Privacy-sensitive changes to reflect relevant portions of privacy compliance documentation; any privacy protection requirements will need to be incorporated in SOPs before SOPs are implemented.

4.0 RFID TECHNOLOGY SECURITY GUIDELINES

This section describes current RFID technologies and their security capabilities. RFID standards, security features, and vulnerabilities are discussed as well. Finally guidelines are presented to ensure that RFID technologies are deployed in a secure manner.

4.1 RFID Technologies

RFID is a technology that enables users to communicate remotely with wireless devices (tags) by electromagnetic signals that identify and track the tags, and thus the objects to which they are attached. An RFID system includes tags, tag readers, local computer hosts, and backend applications and databases. Data on tags is scanned by readers and sent to backend servers; the

entire process can be done automatically, simultaneously, and remotely. Figure 1 depicts a passive RFID system and data flow.

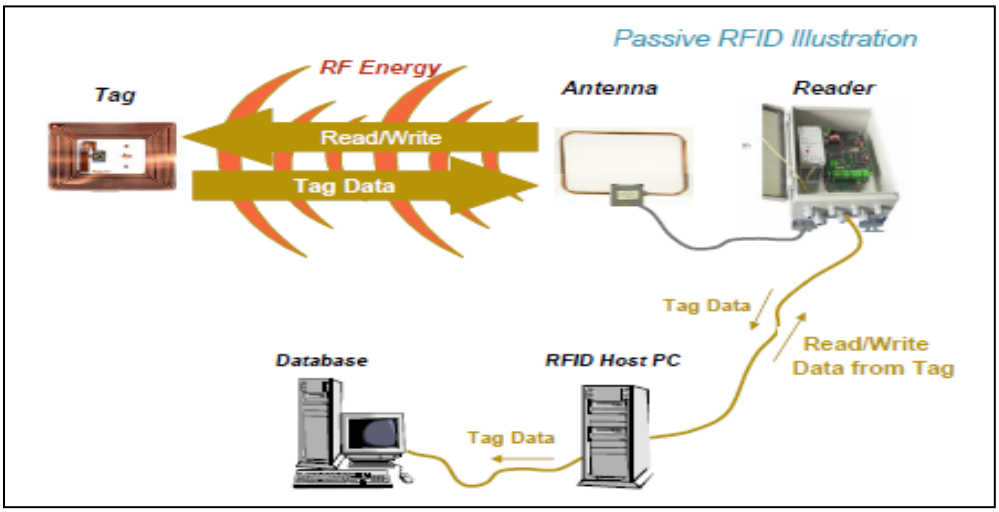

Figure 1: An RFID system and data flow.

Some tags store only simple identification numbers, while others can store more information such as biometric data, location, temperature and humidity, etc., depending on tag hardware capabilities and attached peripheral devices. For example, a special class of location tags uses standard enterprise Wi-Fi networks to track assets and people in real time by combining location and ID information; a typical such system could be used for dynamically tracking wheelchairs in a hospital.

An RFID tag has a small microchip and an antenna. Tags and tag readers communicate using various parts of the electromagnetic spectrum such as low frequency (LF), high frequency (HF), and ultra high frequency(UHF); Wi-Fi; infrared; and ultrasound. In general, two types of RFID tag are used for asset tracking and other purposes: semi-passive and semi-active:

- Passive and semi-passive tags do not have internal energy source and receive energy via RF from external sources such as tag readers
- Active and semi-active tags have internal energy sources and can automatically transmit RF signals to tag readers.

4.2 Active Tag Security

Active tags emit periodic RF signals, and depending on the frequency and transmit power level, the signals can penetrate such objects as walls and travel a long distance. For instance, Wi-Fi tags can be read at a range of a few hundred meters in open space and a range of tens of meters in doors.

Currently, most active tags do not support robust authentication or encryption capability, and data transmitted by active tags can be easily read by eavesdroppers using compatible readers; active tags should therefore be used only within a secure operating environment. It is extremely important for organizations to understand the underlying mechanism of active tags, evaluate the

business and operation requirements, assess the risks and vulnerabilities, and make informed decisions balancing operation and security considerations.

4.3 Passive Tag Security

Currently, the most common passive tag standard is the Electronic Product Code (EPC) Class 1 Generation 2 (Gen 2) standard. This standard is mandated by, for example, DoD and Walmart, and has been widely adopted by both industry and Government organizations. The EPC Gen 2 standard, however, provides only a very limited set of security features:

- A16-bit random number generator for two-way hand-shaking and data masking. First, it is used to track and lock a given tag-reader session to avoid collisions when multiple tags or readers are present. It is also used as a key to perform a trivial encryption of passwords and information written to a tag by a reader when executing the "write" command. It is NOT used for encryption of identification data from a tag to a reader.
- A 16-bit cyclic redundancy check (CRC) for error detection.
- A 32-bit password that is required to perform the "kill" command to disable tags.
- A 32-bit password that is required to access certain parts of tag memory such as password bits for "writing" operations. This password is NOT used for tag ID data access authentication.

All these features are considered cryptographically weak as the bit lengths are short, so the following security risks must be considered when this type of tag is deployed:

- EPC tags respond to any compatible reader without authentication.
- The kill and access control passwords are static and short; they provide only one-way reader-to-tag authentication, and therefore they can be cracked by determined attackers.
- The EPC standard has no data encryption requirement, either on the tags or in the air.
- EPC passwords are cryptographically weak.
- The random number key that is used by readers for masking data transmitted from readers to tags can be intercepted when it is initially transmitted by tags to readers.

Organizations should understand these inherent vulnerabilities associated with the EPC tags, evaluate the business requirements and operation environments, make an informed decision that balances operational and security perspectives, and develop security controls to reduce risks to an acceptable level.

- EPC Class 1 Generation 2 based tags should be used only for asset management only.

Due to the open nature of RFID technologies, tags, readers, and local computer hosts are generally vulnerable to tampering or attacks. The following mitigation strategy is recommended:

- Asset management operations that use EPC Class 1 Generation 2 based tags should be performed in a secured environment so that tags cannot be scanned by unauthorized readers. Note that typical maximum range for EPC Gen 2 tag access is about a few meters.

4.4 Smart Card Security

A smart card has an embedded integrated circuit (IC) for on-board data storage and computing operations and follows either the ISO/IEC 7816 standard for contact cards or the ISO/IEC 14443 standard for contactless cards. A smart card connects to a reader by direct physical contact (contact card) or by remote contactless RF interface (contactless card). With its built-in IC and associated microcontroller, a smart card is capable of storing large amounts of data and performing complex operations. Smart cards include robust security features such as encryption and digital signatures, and interact intelligently with external RFID systems. For example, some contactless cards can encrypt data using the AES algorithm, and can use secret built-in unique keys for mutual authentication according to public key infrastructure (PKI).

Smart cards and RFID systems should provide a mechanism to authenticate one another both before communications are established and periodically during communications, thus mitigating smart card attacks. Digital certificates are often used for this purpose; a shared secret key is another alternative. Smart cards can support data integrity by using FIPS-approved hashing algorithms such as Secure Hash Algorithm 2 (SHA-2).

4.5 Near Field Communication Security

Near Field Communication (NFC) is a wireless technology designed to enable communication between two devices over very close distances (a few centimeters), the range limited by to operating frequency, power consumption, and hardware and software design. NFC allows two devices to establish a communication channel that is specified in the ISO/IEC 18092 and 21481 standards. For instance, two NFC-capable smartphone users can share photos by clicking the photos and moving the phones close together.

Few security features such as authentication or encryption are required by the NFC standards. The unique operating nature of NFC, requiring that two devices be in very close proximity, makes it less vulnerable to threats such as eavesdropping, data modification, or man-in-the-middle attacks. Nevertheless, a secure channel at a higher Open Systems Interconnection (OSI) layer, such as Transport Layer Security (TLS) at the application layer, should be used for sensitive data exchange. In addition, unless required by operations or business considerations, the NFC feature on devices should be disabled by default and enabled manually by users to minimize the potential for data leakage.

4.6 Back-end System Security

The RFID backend system is composed of network components, middleware, and business applications that process ID information. It also shares ID information with other enterprise systems such as supply chain applications; therefore, the backend system is deployed within the trusted enterprise boundary; within this boundary established by the Department are DHS-accredited information systems and components for which DHS typically has direct control for the application of required security controls or the assessment of security control effectiveness. Robust perimeter defense-in-depth strategies are needed to ensure that the RF backend system is effectively protected. Firewall, proxy, and content filtering are some of the tools and methods to secure the enterprise boundary. In addition, an SOP should be written and implemented for security patching and for updating the operating systems and applications associated with the back-end system

4.7 Tag Data Security

Data on tags is vulnerable to various attacks, especially data on less capable classes of tags without robust security features. For example, to track laptops via EPC Gen 2 passive tags, instead of storing sensitive data such as organization codes or employee numbers or product serial numbers on tags, one could use non-descriptive and randomized unique numbers to represent sensitive identification information, and in turn use the more secured RFID backend systems to map them for actual identification. In this way, the tag data will not reveal any sensitive information even if it is captured by unauthorized sources.

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.

4.8 RF Leakage

Depending on the RF bands and device power levels, RF signals from tags and readers can be captured and decoded at ranges from a few centimeters to a few hundred meters.

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

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

5.2 Technical Training

In addition to the security awareness training required by DHS Sensitive Systems Policy Directive 4300A, each employee, before being given access to an RFID system, must specifically know how to operate in a secure manner that will not compromise the RFID system and that will sustain privacy protections.

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 Defense, *Suppliers' Passive RFID Information Guide,*version 15

Department of Homeland Security, *DHS 4300A Sensitive Systems Handbook* v11.0, February 2014.

National Institute of Standards and Technology, SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 2010

National Institute of Standards and Technology, SP 800-98, "Guidance for Securing Radio Frequency Identification (RFID) Systems," April 2007

Online References

National Institute of Standards and Technology , FIPS 140-1 and FIPS 140-2 Cryptographic Modules Validation Lists.

http://csrc.nist.gov/groups/STM/cmvp/validation.html

Smart Card Alliance, "Frequently Asked Questions," http://www.smartcardalliance.org/pages/smart-cards-faq .

APPENDIX B: CHECKLIST FOR SECURING RFID SYSTEMS

RFID SENSITIVE SYSTEM SECURITY CHECKLIST			
✓	**Section 2.1: RFID Usage Policy**	**Required**	**Recom-mended**
	Any Component using RFID technology specifically documents and ensures that the use and users of RFID comply with DHS Sensitive Systems Policy ADirective 4300A and all other related DHS RFID security and privacy policies.	X	
✓	**Section 2.2: Agreements With External Organizations**	**Required**	**Recom-mended**
	Component has instituted 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 such as Department of Defense (DoD), Department of Energy DOE, and Department of State DOS; private individuals; corporations; and non-governmental organizations such as the Red Cross.	X	
	A third party audits compliance with external organization agreements.		X
✓	**Section 2.3: Privacy**	**Required**	**Recom-mended**
	The use of the tags and all associated data is limited to the intended area of operation and is not being used in any way connected with the individual outside that area of operation. This limitation is specifically addressed in the associated privacy compliance documentation and audit table.		X
	Components and third parties are not able to determine an individual's location based on the location of the tag outside the tag's intended area of operation.		X
	Components and third parties are not able to reveal specific information based on a specific tag outside of the tag's intended area of operation		X
✓	**SECTION 3.0: STANDARD OPERATING PROCEDURES**	**Required**	**Recom-mended**
	SOPs are maintained for each of the following areas: 1. Configuration management 2. Security incident response 3. Temporary suspension of security controls 4. Continuity of operations (COOP)	X	
	Each Component maintains separate SOPs for different organizational elements such as divisions and branches, and occasionally for job categories, as long as every organizational element is covered by compliant SOPs.		X
	Each Component submits its SOPs to the WMO so that it may review the SOPs' security procedures and requirements for compliance with DHS Sensitive Systems Policy Directive 4300A .	X	
	Component SOPs are maintained in alignment with privacy compliance documentation as it changes over time.	X	

	SOPs include the following: • Date and version of the SOP • Letter of approval • Contact information for security-related questions about the SOP • Any standard DHS notices or warnings.	X	
✓	**Section 3.1: Physical Access Control**	**Required**	**Recom-mended**
	Components 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	
	Components 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	
	Components use RF shielding on the perimeter of the RFID system implementation.		X
✓	**Section 3.2: Appropriate Placement of RFID Equipment**	**Required**	**Recom-mended**
	Components assess hazards due to electromagnetic radiation, considering hazards of electromagnetic radiation to ordnance (HERO); hazards of electromagnetic radiation to fuel (HERF); and hazards of electromagnetic radiation to personnel (HERP), using the following references for guidance: • 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	
	If HERO/HERF/HERP assessments determine that risks exist, Components have established minimum safe distances, maximum power levels, or duty cycles.	X	
✓	**Section 3.3: Secure Disposal of Tags**	**Required**	**Recom-mended**
	Tags are securely disposed of by physical or electrical means after they have performed their intended task.		X
	All tags used in connection with individuals are securely disposed of after intended task is completed.	X	
✓	**Section 3.4: Separation of Duties**	**Required**	**Recom-mended**
	Separate individuals are assigned to tagging and reading roles of for each RFID system implementation when tagged items are of high value or contain sensitive user or Component information.		X
✓	**Section 3.5: Configuration Management**	**Required**	**Recom-mended**

	The configuration management SOP specifies the membership of the Configurations Control Board (CCB). The CCB membership SHOULD be based on personnel roles rather than named individuals.	X	
	The CCB membership is based on personnel roles rather than named individuals.		X
	The configuration management SOP specifies the procedure by which proposed changes are to 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 at a minimum includes 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.	X	
	The configuration management SOP specifies the voting procedure for CR approval.	X	
	Approval requires unanimous written consent by the CCB membership, either . electronic, by e-mail or by an authenticated entry in a configuration management software tool.		X
	The configuration management SOP specifies an emergency change procedure for any configuration change that needs to occur before a meeting of the CCB in order to restore the availability or security of the system.	X	
	The configuration management SOP requires timely submission of an emergency CR for retroactive approval of each emergency change. .	X	
	The time frame for submission of an emergency CR is no later than 48 hours after the change.		X
	The configuration management SOP requires that the system be rolled back to its state before the emergency whenever an emergency CR is not approved.		X
	The configuration management SOP includes controls related to the appropriate separation of duties.		X
	Individuals who load tags are not permitted to read the tags.		X
	The configuration management specifies the procedure by which technical personnel document the completion of an approved CR. •	X	

	The procedure includes a description of the information that must accompany each after-action report (AR), including 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
	Retirement or disposal of RFID system hardware is considered a configuration change. They SHALL include zeroization or degaussing for RFID system components, and destruction or using a KILL command for RFID tags.	X	
	The configuration management SOP SHALL specify the procedure for sanitizing RFID system components of key material and other sensitive data before disposal.	X	
	Authorized RFID sanitization techniques do not include simple file deletion or tag disposal, but do include zeroization or degaussing for RFID system components, and destruction or using a KILL command for RFID tags.	X	
	The configuration management SOP specifies the recordkeeping requirements for CCB proceedings.	X	
	Approved CRs and approved ARs are maintained for a period not less than 1 year.	X	
	Approved CRs and approved ARs are maintained for the lifetime of the system		X
✓	**3.6 Security Incident Response**	**Required**	**Recom-mended**
	The Security Incident Response SOP specifies methods for RFID system users and other personnel to report security incidents, in accordance with DHS 4300A Sensitive Systems Handbook, Attachment F and NIST Special Publication 800-61, "Computer Security Incident Handling Guide." If the tag is used in connection with individuals, the Security Incident Response SOP includes a requirement to also report incidents to the DHS Privacy Office.	X	

✓	**3.6.1 Radio Frequency Interference**	**Required**	**Recom-mended**
	A site survey is conducted before the deployment of an RFID subsystem to check for radio interference with the planned system.		X
	The security incident response specifies actions to take after radio users detect radio interference, and the specified actions include at a minimum the following: • Notifying a relevant authority that the interference is occurring • Mitigating the impact of the interference by the implementation of shielding or other effective means.	X	
	If radio interference cannot be circumvented, and interference is degrading mission performance, personnel switch to a backup form of asset tracking such as barcodes or paper-based systems.		X

	The security incident response SOP covers procedures for identifying the source of interference by triangulation or other means. If such procedures are included, they include methods of evidence collection that would allow for subsequent prosecution of illegal behavior.		X
	Components receive radio frequency (RF) authorization, if required, 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**	**Required**	**Recom-mended**
	The COOP SOP specifies the roles and responsibilities of personnel during a significant system outage.	X	
	A personnel notification roster is distributed to all relevant personnel for use during emergencies or significant outages.		X
	The COOP SOP lists 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	
	The COOP SOP specifies the circumstances under which personnel should operate backup tracking methods (e.g., when infrastructure connectivity is unavailable).	X	
✓	**3.8 Security Auditing**	**Required**	**Recom-mended**
	The RFID system is configured to create, maintain, and protect an audit trail, which will include the following security-related events, to the extent the technology supports this capability: • Deactivation of a security feature • Successful and unsuccessful login attempts • Access to system administrator functions.	X	
	The auditing process is described as part of the privacy compliance analysis and documentation process to ensure that privacy sensitive data is only and always used appropriately.	X	
	SECTION 4.0: TECHNOLOGY		
✓	**4.3 Passive Tag Security**	**Required**	**Recom-mended**
	EPC Class 1 Generation 2 based tags are used only for asset management only.		X
	Asset management operations that use EPC Class 1 Generation 2 based tags are performed in a secured environment so that tags cannot be scanned by unauthorized readers. Note that typical maximum range for EPC Gen 2 tag access is about a few meters.		X
✓	**4.4 Smart Card Security**	**Required**	**Recom-mended**
	FIPS 140-2 approved AES-256 algorithms are used to secure communications between tags and readers, and data on the tags.	X	
	If the smart cards selected do not support FIPS-approved AES-256 algorithms, then an algorithm is selected according to industry best practices.		X
	Smart cards provide mutual authentication capabilities to ensure that only authorized cards and readers are able to exchange data.		X

	Data integrity capabilities are enabled to ensure that an adversary cannot modify data in either during transactions or at rest.		X
✓	**4.7 Tag Data Security**	**Required**	**Recom-mended**
	Non-descriptive identifiers are used in tags to minimize sensitive information leakage.		X
	Components do not use tags to hold more than a unique identifier unless approved by the AO.		X
✓	**4.8 RF Leakage**	**Required**	**Recom-mended**
	RF survey and assessment are needed to ensure that the RF footprint and device power level are adjusted to minimize the RF leakage. In addition, RFID operations are be performed in a secured environment so that tags cannot be scanned by unauthorized readers.		X
	SECTION 5.0: TRAINING AND EXERCISES		
✓	**5.1 Security Awareness Training**	**Required**	**Recom-mended**
	In accordance with DHS Sensitive Systems Policy Directive 4300A requirements, appropriate security awareness training is provided.	X	
	Any appropriate wireless security awareness training is be included in the annual training provided at the Component level.		X
	Upon completion of the security awareness training for RFID systems, each employee has, at a minimum, knowledge of the following: • The Component'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 (RF) interference ° Broken or tampered-with tag.		X
✓	**5.2 Technical Training**	**Required**	**Recom-mended**
	Each employee's technical training includes 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	
	Newly hired employees have obtained initial technical training before being given them access to RFID systems.	X	
	Technical training courses for system users and system administrators include security- and privacy-related instructions.	X	
	Security and privacy technical training is combined with other technical training related to the RFID system.		X
	Components include training materials as part of their accreditation package.	X	

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

AO	Authorizing Official
CCB	Change Control Board
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CR	Change Request
~~DAA~~	~~Designated Accrediting Authority~~ (obsolete; term replaced by Authorizing Official (AO)
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOS	Department of State
FCC	Federal Communications Commission
HERF	Hazards of Electromagnetic Radiation to Fuel
HERO	Hazards of Electromagnetic Radiation to Ordnance
HERP	Hazards of Electromagnetic Radiation to Personnel
HF	High Frequency
IA	Information Assurance Identification and Authentication
ISA	Interconnection Security Agreement
LF	Low Frequency
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
OCIO	Office of the Chief Information Officer
OET	Office of Engineering and Technology (of the FCC)
OMB	Office of Management and Budget
OPSEC	Operations Security
OSM	Office of Spectrum Management

RF	Radio Frequency
RFID	Radio Frequency Identification
SHA-2	Secure Hash Algorithm 2
SOP	Standard Operating Procedures
SP	Special Publication Security Plan
TLS	Transport Layer Security
UHF	Ultra High Frequency