U.S. Customs and Border Protection

HB 1400-05D

Information Systems Security Policies and Procedures Handbook

Office of Information and Technology

Cybersecurity Directorate

Version 8.0

September 13, 2024

DOUGLAS S DAVIS

Digitally signed by DOUGLAS S DAVIS
Date: 2024.09.18 12:18:15 -04'00'

Table of Contents

Introduction ... 6
Security Objectives ... 6
IT Security Program Policy and Implementation Guidelines ... 6
Applicability ... 7
Authorities and References ... 7
Information Systems Security Policy Hierarchy ... 12
Policy Overview ... 13
Changes to Policy ... 13
Offenses and Penalties ... 13
1.0 General CBP Security Policy ... 14
2.0 Roles and Responsibilities ... 20
2.1 Commissioner ... 21
2.2 Executive Assistant Commissioner, Enterprise Services ... 22
2.3 Assistant Commissioner, Officer of Information Technology ... 22
2.4 Authorizing Official ... 22
2.5 Chief Financial Officer ... 24
2.6 Chief Information Officer ... 24
2.7 Financial System Owners ... 25
2.8 Other Assistant Commissioners ... 25
2.9 Chief Information Security Officer ... 26
2.10 Information System Security Manager ... 27
2.11 Security Control Assessor ... 28
2.12 Certification Agent ... 28
2.13 Information System Security Officer ... 29
2.14 Supervisors and Managers ... 32
2.15 Privacy Officer ... 33
2.16 Program Managers ... 33
2.17 Information System Owners and Information Owners ... 34
2.18 System and Network Administrators ... 35
2.19 System Control Officer ... 36
3.0 Management Policies ... 36

3.1 Capital Planning and Investment Control 36
3.2 Contractors and Outsourced Operations 37
3.3 System Engineering Life Cycle 39
3.4 Configuration Management 39
3.5 Security Authorization and Security Control Assessments 39
3.6 Privacy Sensitive Systems 43
3.7 E-Authentication 43
3.8 CFO Designated Financial Systems 43
4.0 Operational Controls 44
4.1 Personnel 44
4.1.1 Citizenship, Personnel Screening, and Position Categorization 44
4.1.2 Segregation of Duties 46
4.1.3 Information Security and Privacy Awareness Training 47
4.2 Personal Use of Government Equipment and DHS/CBP Systems 48
4.3 Physical Security 49
4.4 Production, Input, Output/Information Handling 50
4.5 Hardware and Software 52
4.6 Storage Media 53
4.7 Removable Media 54
4.8 Voice Communication Security 55
4.9 Wireless Communications 55
4.9.1 Wireless Mobile Devices 56
4.10 Wireless Settings for Peripheral Equipment 58
4.11 Wireless Input Peripheral Devices 59
4.12 Personally Owned Equipment and Software 60
4.13 DHS and CBP Information Security Operations 62
4.14 Vulnerability Management 63
4.15 Information and Data Backup 64
4.16 Backup Strategy 67
4.17 Local Area Network Guidance 68
4.18 Converging Technologies 69
5.0 Technical Policies 71
5.1 Identification and Authentication 71

5.2 Access Control ... 75
5.2.1 Automatic Account Lockout ... 78
5.2.2 Automatic Session Termination ... 79
5.2.3 Warning Banner ... 80
5.2.4 External User Account Recertifications ... 82
5.3 Auditing ... 83
5.4 Network and Communications Security ... 87
5.4.1 Remote Access and Dial-In ... 87
5.4.2 Network Security Monitoring ... 92
5.4.3 Network Connectivity ... 95
5.4.3.1 Interconnection Security Agreements ... 99
5.4.3.2 Trust Zones ... 100
5.4.4 Firewalls and Policy Enforcement Points ... 102
5.4.5 Router Device Management ... 109
5.4.6 Internet Security ... 110
5.4.7 Email Security ... 121
5.4.8 Personal Email Accounts ... 127
5.4.9 Group Mailing ... 128
5.4.10 Testing and Vulnerability Management ... 129
5.4.11 Peer-to-Peer Technology ... 133
5.5 Scanning and Monitoring Policy ... 135
5.5.1 Authorized/Approved Monitoring ... 137
5.5.2 Sniffer Devices ... 139
5.6 Cryptography ... 139
5.6.1 Encryption ... 140
5.6.2 Public Key Infrastructure ... 142
5.6.3 Public Key/Private Key ... 150
5.7 Malware Protection ... 154
5.7.1 What Is a Virus? ... 156
5.7.2 Types of Malware ... 156
5.7.3 How Malware Affects Systems ... 157
5.7.4 Procedures When Malware Is Detected on a System ... 157
5.8 Product Assurance ... 158

5.9 Supply Chain 160
5.9.1 Business Impact 162
5.9.2 Supply Chain Risk Management Plans 162
Document Change Requests 170
Questions and Comments 170
Definitions 170
Attachments 174

Introduction

U.S. Customs and Border Protection (CBP) must incorporate security safeguards within its information systems to support the DHS mission. This handbook serves as an aid to CBP Information Technology (IT) users to achieve confidentiality, integrity, availability, and non-repudiation within CBP IT infrastructure and operations. This handbook is based on DHS 4300A Information Technology System Security Program, Sensitive Systems Policy Directive and provides supplemental policy for CBP-specific mission needs. In addition, it implements as requirements many of the guidelines contained in various National Institute of Standards and Technology (NIST) publications, Office of Management and Budget (OMB) direction, Congressional and Executive Branch mandates. Due to its business mission, CBP systems may require policies and procedures that are more stringent than those required by federal or DHS security policy.

The intended audience includes all elements of CBP using information systems and networks within CBP. Specific procedures supporting these policies may be found in the attachments. The scope and contents of this handbook will change over time as new capabilities are added to CBP systems, as security standards are upgraded, and as a result of user experience and comment. This handbook is issued as implementation guidance under the authority of the Chief Information Officer (CIO) through the Chief Information Security Officer (CISO). This handbook addresses IT security only. However, those aspects of personnel, physical, information, and industrial security; investigations; emergency preparedness; and counterterrorism that relate to IT security are addressed in this handbook.

Security Objectives

Confidentiality, availability, integrity, and non-repudiation are the CBP primary security objectives. A framework is provided to develop security policies and procedures for CBP. Risk Management is another key objective, which is addressed in more detail in Section 3.8, Risk Management. The weighing of risks associated with each primary security objective may not be equal, nor will it be assessed in the same way for classified, Sensitive but Unclassified (SBU) information, and information systems at CBP. Federal Information Processing Publication (FIPS) -199, Standards for Security Categorization of Federal Information and Information Systems, offers guidance to categorize information systems based on the priority of each of the security objectives. CBP follows this guidance in categorizing its SBU information and information systems.

IT Security Program Policy and Implementation Guidelines

This handbook provides procedures and techniques necessary to implement the Baseline Security Requirements (BLSRs) relating to management, operational, and technical controls that provide the foundation necessary to ensure confidentiality, integrity, availability, authenticity, and non-repudiation within the CBP IT infrastructure and operations. This handbook addresses the procedures necessary for implementing security requirements for sensitive IT systems. A CBP system is any information system that

transmits, stores, or processes data or information and is (1) owned, leased, or operated by CBP, (2) operated by a contractor on behalf of CBP, or (3) operated by another Federal, state, or local Government agency on behalf of CBP. CBP policy mandates that all CBP computing resources be individually accounted for as part of an IT system. IT systems encompass major applications and general support systems.

The CBP Information Security Program does not apply to any IT that processes, stores, or transmits foreign intelligence information pursuant to Executive Order 12333, to Director of Central Intelligence directives governing the protection of intelligence information, and to other applicable orders.

Policy elements are effective when issued. Failure to implement any policy element within 135 business days shall be considered a weakness and either a system or program Plan of Action and Milestones (POA&M) must be generated by the organization for the identified weaknesses.

Applicability

This handbook applies to all CBP personnel, contractors acting for CBP, and all authorized users who access CBP information systems. The CBP Information Systems Security Policies and Procedures Handbook apply to all CBP information systems used to process, store, transmit, or receive any CBP data.

CBP Mission Statement

Information security principles and practices in this document support the basic CBP mission stated below:
We are the guardians of our Nation's borders. We are America's frontline.
We safeguard the American homeland at and beyond our borders.
We protect the American public against terrorists and the instruments of terror.
We steadfastly enforce the laws of the United States while fostering our Nation's economic security through lawful international trade and travel.
We serve the American public with vigilance, integrity, and professionalism.

Authorities and References

DHS established a department-wide IT security program presented in DHS 4300A *Information Technology System Security Program, Sensitive Systems Policy Directive* and DHS 4300B *National Security Systems Handbook* for classified systems. These policies and authorities extend to CBP, a component of DHS.

Applicable Executive Orders, public laws, national policy, external/internal guidance and DHS direction for this handbook include the following:

Public Law and U.S. Code

- Public Law 100-235, Computer Security Act of 1987 as amended
- Public Law 101-576, Chief Financial Officers (CFO) Act of 1990

- Public Law 104-106, Clinger-Cohen Act of 1996, 40 U.S.C. 1401 (formerly, Information Technology Management Reform Act of 1996 (ITMRA))
- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Freedom Act of 2002 as amended
- Public Law 106-398, *National Defense Authorization Act of 2001*
- Public Law 107-296, Homeland Security Act of 2002
- Public Law 107-347, E-Government Act of 2002.
- Public Law 113-283, 128 STAT 3073 Federal Information Modernization Act of 2014
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch

Executive Orders

- Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities*, dated November 18, 1988, as amended
- Executive Order 13200, President's Information Technology Advisory Committee, Further Amendment to Executive Order 13035, as Amended, Signed: February 11, 2001
- Executive Order 13215, President's Information Technology Advisory Committee, Further Amendment to Executive Order 13035, as Amended, Signed: May 31, 2001
- Executive Order 13228, Establishing the Office of Homeland Security and the Homeland Security Council, Signed: October 8, 2001
- Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001
- Executive Order 13526, Classified National Security Information, December 29, 2009
- Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003
- Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004
- Executive Order 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*, July 6,2012

Office of Management and Budget (OMB) Directives

- OMB Bulletin 24-02, *Audit Requirements for Federal Financial Statements,* July 29, 2024
- OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E- Government Act of 2002*, September 2003
- OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies,* December 16, 2003
- OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006

- OMB Memorandum M-06-16, *Protection of Sensitive Agency Information,* June 23, 2006
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* May 22, 2007
- OMB Memorandum M-09-02, *Information Technology Management Structure and Governance Framework,* October 21, 2008.
- OMB Memorandum 10-15, *FY 2010 Reporting Instructions for the Federal Information*
- *Security Modernization Act of 2014 and Agency Privacy Management*, April 21, 2010
- OMB Memorandum 11-06, *WikiLeaks – Mishandling of Classified Information*, November 28, 2010
- 9/11 Act of 2007, Increased Mission Requirements for Chief Privacy Officer
- OMB Circular A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004
- OMB Circular A-130, *Management of Federal Information Resources,* July 28,2016

Other External Guidance

- Intelligence Community Directive Number 503, *Intelligence Community Information Technology Systems Security Risk management, Certification and Accreditation*, September 15, 2008
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS), including:
    - FIPS 140-3, *Security Requirements for Cryptographic Modules*. March 2019
    - FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
    - FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006
- NIST Information Technology Security Special Publications (SP) 800 series, including:
    - NIST SP-800-18, *Guide for Developing Security Plans for Information Technology Systems, Revision 1,* February 2006
    - NIST SP-800-30, Rev 1, *Guide for Conducting Risk Assessments*, September 2012
    - NIST SP-800-34, Rev 1, *Contingency Planning Guide for Information Technology Systems,* November 2010
    - NIST SP-800-37, Rev 2*, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, December 2018

- NIST SP-800-39, *Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View*, March 2011
- NIST SP-800-47, Rev. 1*, Managing the Security of Information Exchanges,* July 2021
- NIST SP-800-50, Rev. 1, *Building a Cybersecurity and Privacy Learning Program,* September 2024
- NIST SP-800-53, Rev. 5*, Security and Privacy Controls for Information Systems and Organization,* December 2020
- NIST SP-800-53A, Rev. 5. *Assessing Security and Privacy Controls in Information Systems and Organizations,* January 2022
- NIST SP-800-53B, *Control Baselines for Information Systems and Organizations*, December 2020
- NIST SP-800-55, Rev 1, *Performance Measurement Guide for Information Security,* July 2008
- NIST SP-800-60 Rev. 2*, Guide for Mapping Types of Information and Systems to Security Categories (Draft)*
- NIST SP-800-60 Vol. 1 Rev. 1*, Guide for Mapping Types of Information and Information Systems to Security Categories,* August 2008
- NIST SP-800-60 Vol. 2 Rev. 1*, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices,* August 2008
- NIST SP-800-61, Rev. 2*, Computer Security Incident Handling Guide,* August 2012
- NIST SP-800-63-3*, Digital Identity Guidelines,* March 2020
- NIST SP-800-63A*, Digital Identity Guidelines: Enrollment and Identity Proofing,* March 2020
- NIST SP-800-63B*, Digital Identity Guidelines: Authentication and Lifecycle Management,* March 2020
- NIST SP-800-63C*, Digital Identity Guidelines: Federation and Assertions,* March 2020
- NIST SP-800-88, Rev. 1*, Guidelines for Media Sanitization,* December 2014
- NIST SP-800-92 Rev. 1*, Cybersecurity Log Management Planning Guide,* October 2023
- NIST SP-800-94*, Guide to Intrusion Detection and Prevention Systems (IDPS),* February 2007
- NIST SP-800-95, *Guide to Secure Web Services,* August 2007
- NIST SP-800-98*, Guidelines for Securing Radio Frequency Identification (RFID)Systems,* April 2007
- NIST SP-800-100*, Information Security Handbook: A Guide for Manager,* March 2007
- NIST SP-800-115*, Technical Guide to Information Security Testing and Assessment,* September 2008

  - NIST SP-800-122, *Guide to Protecting the confidentiality of Personally Identifiable Information (PII),* April 2010
  - NIST SP-800-123*, Guide to General Server Security,* July 2008
  - NIST SP-800-124 *Rev. 2, Guidelines for Managing the Security of Mobile Devices in the Enterprise,* May 2023
  - NIST SP-800-128, *Guide for Security-Focused Configuration Management of Information Systems,* October 2019
  - NIST SP-800-137, *Information Security Continuous Monitoring for Federal*
  - *Information Systems and Organizations,* September 2011
  - NIST SP-800-175A, *Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies*
  - NIST SP-800-175B, *Rev. 1, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*
- NIST IR 7298, *Glossary of Key Information Security Terms*
- CNSS Instruction No. 4009, *National Information Assurance Glossary*
- CNSS Instruction No. 1001, *National Instruction on Classified Information Spillage*
- Code of Federal Regulations (CFR) §2635, *Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch*

Departmental/Agency Policy

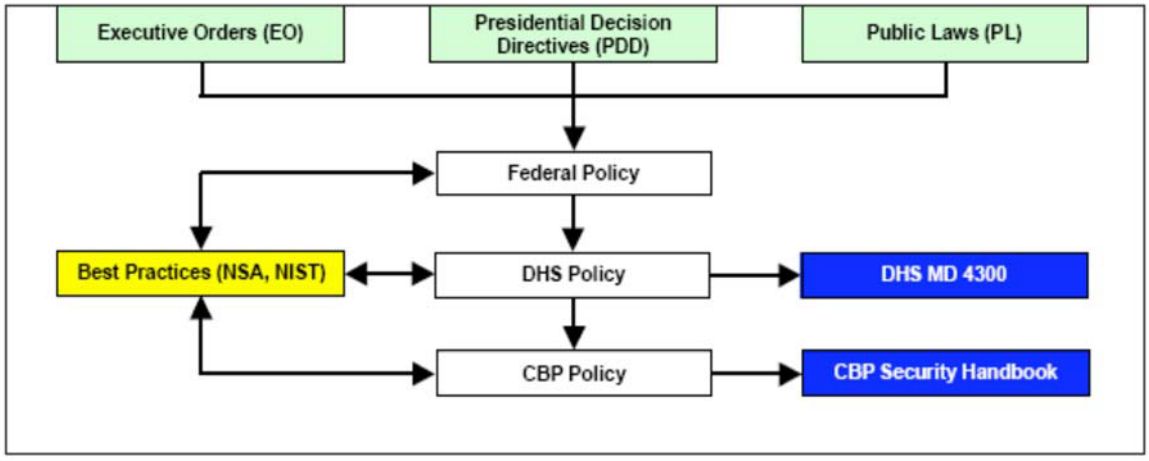
- Department of Homeland Security Acquisition Regulation (HSAR)
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000
- DHS Management Directives (e.g., MD 0470.1, MD 102-01, MD 140-01, MD 1030, MD 4400.1, MD 4500.1, MD 4600.1, MD 4900, MD 11042.1, MD 11050.2)
- Federal Financial Management Improvement Act of 1996 (FFMIA), P.L. 104-208
- Federal Managers' Financial Integrity Act of 1982 (FMFIA), P.L. 97-255
- The National Security Act of 1947, dated July 26, 1947
- DHS Policy Directive 4300A: Information Technology System Security Program, Sensitive Systems, February 2023
- DHS, IT Security Procedural Guide, Developing a Contingency Plan (Appendix 1 of DHS Security Program Handbook)
- CBP, System Life Cycle Handbook, CIS HB 5500-07B, Version 1.2, October 16, 2008
- Department of Defense Directive 8100.2, April 14, 2004, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)
- CBP Directive No. 1450-26 Use of Secure Messaging Platforms, June 29, 2023
  - Annex A, Use of Secure Messaging Service and Multimedia Messaging Service; Limited Use of Personal Devices, August 28, 2024
- CBP Records Information Management (RIM) Directive, 2210-040, January 3, 2019

- CBP RIM Handbook, HB2100-05B, Version 1.0, June 3, 2019
- Capstone Email Policy, January 2021
- CBP RIM Program Annex D: Essential Records and Databases, Version 1.0, September, 18, 2020
- Minimum RIM Requirements for Electronic Information System (EIS), Version 1.0, January 2023 CBP RIM SharePoint site

Information Systems Security Policy Hierarchy

Federal security policy flows from the executive level and Public Law to Department and Bureau levels. Development of policy at the national level generally begins with the creation of an Executive Order (EO), a Presidential Decision Directive (PDD), or a Public Law (PL). Other organizations such as the National Security Agency (NSA), the National Institute of Standards and Technology (NIST), and OMB also provide guidance and directives for policy development. Federal agencies use these orders, directives, laws, and guidance to generate policies and practices applicable to their organizations. Figure 1.6, Security Policy Development depicts the flow of points of policy origination for CBP

Figure 5.1: Security Policy Development



Policy Overview

Security of federal information systems is mandated by law (see *References*). Information security policy regulates how an organization protects and assigns resources to achieve its security objectives. Security safeguards and countermeasures are selected as a result of risk assessment activities. The overall CBP information technology security program encompasses the architectural framework that contains applications, networks, hardware, software, services, processes, policies, documentation, and resources that assist in accomplishing the CBP mission. Funding of CBP is closely tied to the robustness of its security program, which must be reported annually to OMB. Great importance is given to security authorization of applications and systems. Security status of a project is weighted heavily in Congressional funding considerations. Section II.B of the OMB Exhibit 300 annual report, requires detailed reporting on the security program.

CBP IT security policies delineate the security management structure and foundation to ensure adequate control over DHS sensitive information and systems. Policies in this document are organized under three areas: management, operational, and technical.

- **Management controls -** Focus on managing both system information security system and system risk. These controls consist of risk mitigation techniques and concerns normally addressed by management.
- **Operational Controls –** Focus on mechanisms primarily implemented and executed by the people responsible for the use of the system. These controls are designed to improve security or a particular system or group of systems. These controls require technical or specialized expertise and often rely on management and technical controls.
- **Technical Controls –** Focus on security controls executed by the information systems. These controls provide automated protection from unauthorized access or misuse. They facilitate detection of security violations, and support security requirements for applications and data.

Changes to Policy

Procedures and guidance for implementing this policy are outlined in a companion publication and DHS 4300A Sensitive Systems Handbook and its attachments. The Handbook serves as the foundation for Components to use in developing their information security programs. However, there are additional policy areas addressed within the 1400-05D that are not addressed by DHS or are addressed more strictly than the DHS 4300A policy. For clarification of CBP information security policies or change requests, cyber.training.policy@cbp.dhs.gov.

- The CBP CISO is the authority for interpretation, clarification, and modification of the CBP 1400-05D Handbook (inclusive of all appendices and attachments).
- The CBP 1400-05D is reviewed at least annually.

Offenses and Penalties

All users authorized to access CBP systems are responsible for complying with the policies in this handbook, as well as other CBP policies that govern standards of behavior within CBP.

Failure to comply with these policies subjects a violator to the published penalties. Supervisors and managers are responsible for determining appropriate disciplinary action and applicable penalties for violations. Although some infractions may incur progressive disciplinary actions, others may be serious enough to warrant removal. Refer to the CBP Table of Offenses and Penalties for more information.

1.0 General CBP Security Policy

All information technology that generates, stores, processes, transfers, or communicates sensitive information shall be protected at a level commensurate with the threat. The following security practices, therefore, are necessary:

1. New system acquisitions, system development, and modifications to existing systems must be coordinated with the Office of Information and Technology Cybersecurity Directorate
2. It is recommended that a label be affixed to media containing Sensitive-But-Unclassified (SBU) information, especially in environments where both sensitive information and classified information are processed. Labels stating "this medium is unclassified" are available from General Services Administration (GSA) Standard Form (SF) 710. Unless otherwise specified, SBU data should be labeled as "For Official Use Only" and safeguarded against unauthorized disclosure, modification, access, use, or destruction. (See Table *Information Handling Policies by Classification Level* for details.)
3. All Major Applications (MAs) and General Support Systems (GSSs) must be authorized to comply with required security controls.
4. Connections between CBP information systems and any other systems or networks not under CBP authority are unauthorized, unless documented by a formally approved Interconnection Security Agreement (ISA) signed by the CBP Chief Information Security Officer (CISO). The non-CBP signatory representative(s) must have the authority to accept the system risk incurred by the connection to CBP. One non-CBP signatory authority would belong to the organization owning the information system and the point of connection to CBP. The organization that owns the data to be transferred through the interconnection may also be a stakeholder in the interconnection. Therefore, an induvial from one or more organizations participating in the interconnection (e.g., the system owner and the data owner) may be the signatory authorities representing the non-CBP side of the connection. Because non-CBP organizations are participants in the ISA and are required to sign the agreement, CBP may have to be somewhat flexible in adhering to the ISA Template. The Information System Security Officer (ISSO) assigned to the system should be contacted before any modifications to the template are made.
5. CBP information systems are for authorized CBP business only.
6. Appropriate physical administrative, and technical safeguards will be implemented and maintained to ensure the most cost-effective security safeguards exist. These safeguards will be consistent with the approved CBP enterprise architecture to ensure proper integration and interoperability,

7. Installation of assistive software, hardware, or other adaptive devices is subject to standard CBP security testing and change request processes before introducing these products to the production environment. Such adaptive devices and/or software must not degrade or circumvent established system security controls.
8. The requirement to protect privacy information is a federal law. CBP systems of record will be afforded the level of security protection commensurate with the level of safeguards required by Federal Privacy Law. For more information on Privacy Law implementation within CBP, contact the Privacy and Diversity Office, Privacy Division.
9. Users have no expectation of privacy when using CBP network resources, including the use of electronic messaging, internet, and other CBP applications and systems. Acceptance of this condition is positively validated when users log onto the network.
10. Security of Non-CBP Sites:
    Organizations providing contracted services to CBP at other than CBP facilities must adhere to the security policies described within this document to include federal policies and regulations. Services provided by non-CBP sites are integral parts of CBP MAs or GSSs and must be considered within the system boundaries of the security authorization process of the applicable information system.
    All CBP information systems must be properly authorized. The Assistant Commissioner, OIT must authorize information systems that are functionally owned and managed by CBP. Any CBP information system operating without the approval of the Assistant Commissioner, OIT is not considered accredited, regardless of any other security authorization, unless there is an explicit written Memorandum of Understanding (MOU) that provides a different policy.
    Non-CBP sites are subject to the same security review as government owned or controlled sites. The reviews are conducted in accordance with FISMA, which states:
    "The head of each agency shall be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of the agency." (H.R. 2458—51, section 3544).
    The goal of the information system security review effort is to ensure that sensitive CBP information being processed at non-CBP facilities is appropriately protected commensurate with federal law, CBP policies, DHS regulations, and security best practices. The objectives of the security reviews are to assess the effectiveness of security controls in place at all facilities, identify areas of strength and weakness, assist in corrective measures, and issue resolution where necessary. Guidance for a self-evaluation of the security controls implemented to protect CBP information systems (i.e., MAs and GSSs as listed in the CBP system inventory) compliance with CBP security policy. The self-assessment used by CBP is found in the NIST SP 800-53, which provides a detailed checklist for 17

security areas. STP staff, namely the ISSOs will complete the self-assessment templates generated by the DHS IACS. Based on DHS requirements, artifacts produced by security reviews of government or contractor/consultant facilities will be completed for each MA or GSS system, but not necessarily for each individual site. Independent audit agencies may validate the results of the completed self-assessments of CBP information systems.

11. **Digital and Other Electronic Signatures**, the following DHS Policy Statements are applicable to both digital signatures and other electronic signature methods.

Policy ID	CBP Policy Statement	Relevant Controls
1.0a	Digital signatures or other electronic signature methods are used whenever practical, except where handwritten signatures are required by law, regulation, Executive Order, or other agency requirement. Digital signature or other electronic signature methods, when properly executed, shall be accepted to the maximum extent practicable.	---
1.0b	When implementing legally binding signatures for a particular application using digital signatures or other electronic signature methods, the participants (signers and relying parties) ensure that they are implemented with an adequate level of security to reduce the risk of malfeasance and/or fraud to an acceptable level, so that the alleged signer or an interested third party cannot: 1) Repudiate that they signed it 2) Deny any intent to sign 3) Challenge the integrity of the signed content	---
1.0c	When a signature is required on electronic documents, transactions, communications, etc. for use within DHS, or for use for intra-governmental transactions, communications, etc., where all potential signers possess a Personal Identity Verification (PIV) card, Department of Defense (DoD)-issued Common Access Card (CAC), or PIV-I card (and the associated card readers, software, and verification processes are in place), the signing process employs a digital signature created by a properly identified signer through the use of their PIV card, CAC issued by DoD or PIV-I card, whenever possible. Signers may use their software-based digital signature certificate that meets the requirements specified in Section 1.12.2.a below, for signing, when their PIV card, DoD-issued CAC, or PIV-I card cannot be used. Other electronic signature methods may be used when it is	---

	determined that it is not possible for the signer to use his/her PIV card, DOD-issued CAC, PIV-I card, or software-based digital signature certificate that meets the requirements specified in Section 1.12.2.a below. Users should consult their legal counsel when primary authentication methods are unavailable.	
1.0d	The following requirements are met when implementing legally binding signatures using Digital Signature or an Other Electronic Signature Method: 1) The Signer uses an acceptable electronic form of signature 2) The electronic form of signature is executed or adopted by a person with the intent to sign the electronic record 3) The electronic form of signature is attached to or associated with the electronic record being signed 4) There is a means to identify and authenticate a particular person as the signer 5) There is a means to preserve the integrity of the signed record.	---
1.0e	Minimally, all electronic correspondence and official digital documents need a digital signature except where a wet signature is required. Electronic signatures, including digital signatures, are implemented by applications with the necessary security controls and practices such that: 1. The signer cannot successfully repudiate that he/she intended to sign, or that he/she applied the electronic signature; and 2. The integrity of the signed content cannot be successfully challenged. Refer to DHS 4300A Attachment Z "Electronic Signature Use, Acceptance, and Implementation Guidance" for further details.	---
1.0f	When implementing legally binding electronic signatures for a specific use, where Other Electronic Signature Methods are used, the risk assessment process, described in the "DHS Electronic Signature Policy Guidance" document, Section I.G. "Determining Which Electronic Signature Method to Use - Risk Assessment and Cost-Benefit Analysis", are used to determine the overall level of risk, and the specific approaches to be implemented to meet each of the following five requirements for legally binding signatures: 1) The Signer uses an acceptable electronic form of signature; 2) The electronic form of signature is executed or adopted by a person with the intent to sign the electronic record; 3) The electronic form of signature is attached to or associated	---

	with the electronic record being signed; 4) There is a means to identify and authenticate a particular person as the signer; 5) There is a means to preserve the integrity of the signed record.	
1.0g	The date and time that a legally binding signature is executed, using Digital Signature or an Other Electronic Signature Method, is captured and incorporated as part of the record of the signature. The captured date and time are accurate and trustworthy. Within DHS, legally binding signatures using a digital signature or other electronic signature method shall be executed on systems whose system clocks have been synchronized via Network Time Protocol (NTP) with DHS networks, and are managed to prevent unauthorized changes to the system clock. When the signature is executed, the date and time from the system clock are captured and incorporated as part of the record of the signature. When a legally binding signature is executed on a system whose system clock is not synchronized via NTP and managed to prevent unauthorized changes to the system clock, the signer is responsible for ensuring that the date and time incorporated as part of the record of the signature is accurate.	---
1.0h	The visual context of an electronic signature implemented using digital signature or other electronic signature method, shall be maintained. The Relying Parties for the electronically signed document, transaction, communication, etc., can view the exact format and content of the document, transaction, communication, etc. that the Signer saw when he or she signed it.	---
1.0i	Where a DHS entity is the Relying Party for an electronic signature executed on a non-DHS system by an external signer, using a digital signature or other electronic signature method, the DHS entity determines whether the asserted signing date and time is sufficiently accurate and trustworthy to be acceptable for the intended use of the signature.	---
	Electronically signed records are maintained based on operational needs, perception of risks, and historical value, as formalized through corresponding Records Disposition Schedules approved by the National Archives and Records Administration (NARA). Operational needs are determined on the basis of the approach taken to ensuring the availability, accessibility, and trustworthiness of electronically signed records	

	over time.	
1.0j	The CISO approves the design, development, resources and infrastructure for implementations of electronic signatures using Digital Signatures or Other Electronic Signature Methods. The adoption and integration of legally binding electronic signature capabilities into workflows, business processes, specific document types, etc., shall be reviewed and approved by CBP General Counsel and by the CBP Chief Records Officer. Additional review/endorsement by other cognizant officials (e.g., PO; Chief Financial Officer; Forms Management Officer; etc.) is obtained when appropriate.	---
1.0k	All implementations of digital signatures or other electronic signature methods in DHS comply with the requirements of DHS Sensitive Systems Policy Directive 4300A. Existing (legacy) implementations of electronic signatures are brought into compliance with DHS Sensitive Systems Policy Directive 4300A as soon as is practical, but in no case later than 12 months, or a waiver is obtained. Waivers are requested in writing and submitted to the DHS CISO.	---

Information Sharing and Communication Strategy

The DHS Security Operations Center (SOC) exchanges information with CBP and other Component SOCs, Network Operations Centers (NOCs), the Homeland Secure Data Network (HSDN) SOC, the Intelligence Community, and with external organizations in order to facilitate the security and operation of the DHS network. This exchange enhances situational awareness and provides a common operating picture to network managers. The operating picture is developed from information obtained from "raw" fault, configuration management (CM), accounting, performance, and security data. This data is monitored, collected, analyzed, processed, and reported by the NOCs and SOCs.

The DHS ESOC is responsible for communicating other information such as incident reports, notifications, vulnerability alerts and operational statuses to the CBP SOC, CBP CISO, or other identified CBP points of contact.

The DHS ESOC portal implements role-based user profiles that allow CBP to use the website's incident database capabilities. Users assigned to CBP groups shall be able to perform actions such as:

- Entering incident information into the DHS ESOC incident database
- Generating preformatted incident reports
- Initiating queries of the incident database
- Viewing FISMA incident reporting numbers

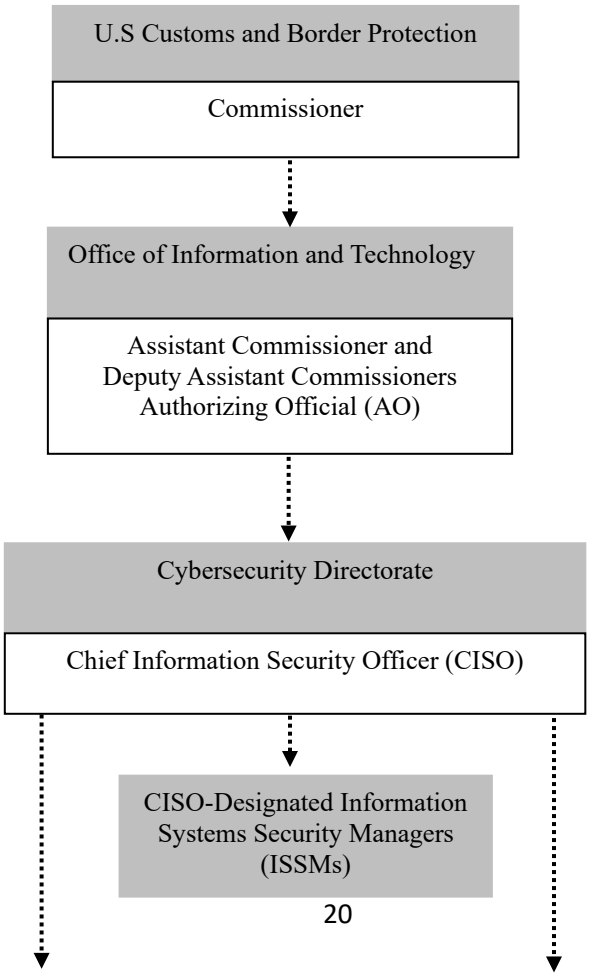
- Automating portions of the Information Security Vulnerability Management (ISVM) program
- Automating portions of the vulnerability assessment program

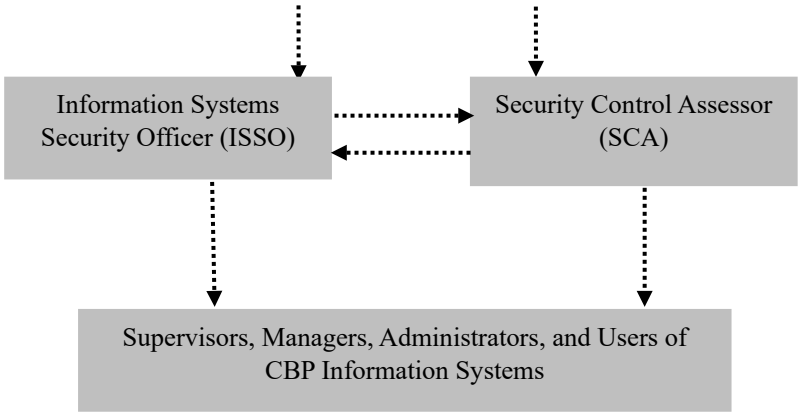
2.0 Roles and Responsibilities

The following roles and responsibilities are detailed in 4300A:

- Authorizing Official (AO)
- Chief Financial Officer (CFO)
- Chief Information Security Officer (CISO)
- Certification Agent (CA)
- Information Systems Security Manager (ISSM)
- Information Systems Security Officer (ISSO)
- Privacy Officer
- Security Accessor

Figure 2.0 Security Management Roles and Responsibilities depict security responsibility relationships and key roles within the CBP Information Security Program.





2.1 Commissioner

The Commissioner of CBP is responsible for all CBP systems and the associated responsibilities described below cannot be delegated. However, the Commissioner's operational authority for the CBP Information Security Program is delegated to the Assistant Commissioner (AC), Office of Information and Technology (OIT). The Assistant Commissioner, OIT is an Authorizing Official for CBP information systems. The Commissioner's responsibility includes ensuring that all information, classified or unclassified, and all CBP automated information systems and their data are protected in accordance with congressional and presidential directives.

Policy ID	CBP Policy Statement	Relevant Controls
2.1	The CBP Commissioner ensures that information systems and their data are sufficiently protected.	PL-1

Within the Department of Homeland Security (DHS) security structure, the CBP Commissioner will:

1. Establish, maintain, and oversee the CBP Information Security Program including its security authorization process program. This responsibility includes the highest level of security management oversight of the development and implementation of all new or substantially modified CBP systems.
2. Appoint the Assistant Commissioner, OIT as one of the Authorizing Officials of CBP. Authority is delegated in writing to the AO to approve or disapprove the operation of all systems functioning within CBP. The Deputy Assistant Commissioner will also be an Authorizing Official of CBP.
3. Appoint Chief Information Officers (CIOs), as documented in DHS security policy.
4. Appoint in writing the Executive Director, Cyber Security Directorate, as the CISO of CBP.

5. Assess and report annually the adequacy of the CBP Information Security Program to the DHS CISO.
6. Ensure that security of CBP information systems is an integral part of the life cycle management process.
7. Ensure that performance measurement requirements are implemented into management of the CBP security program.
8. Establish a SOC with an interface to DHS Computer Emergency Readiness Team (CERT) and CISA.
9. Establish a centralized program for information systems security education, training, and awareness.
10. Ensure that organizations plan, budget, allocate, and spend adequate resources in support of information systems security.
11. Ensure data for IT systems are entered into the appropriate DHS Security Management Tool to support DHS IT security oversight and Federal Information Security Modernization Act of 2014 (FISMA) reporting requirements.

2.2 Executive Assistant Commissioner, Enterprise Services

Executive Assistant Commissioner, Enterprise Services, responsible for integrating and coordinating CBP's mission support functions, including CBP's hiring, budget and acquisition activities.

2.3 Assistant Commissioner, Officer of Information Technology

The Assistant Commissioner, OIT is appointed in writing by the Commissioner. The Assistant Commissioner, OIT is an Authorizing Official (AO) and has the authority to assume formal responsibility on behalf of the Commissioner for operating all CBP systems at an acceptable level of risk. The Assistant Commissioner, OIT may authorize all CBP information systems and accept risk for the security posture of the data and systems. The Deputy Assistant Commissioner is also an Authorizing Official with the same authority. Within the CBP security structure, the OIT Assistant Commissioner is also the Chief Information Officer (CIO) for CBP.

2.4 Authorizing Official

CBP has three Authorizing Officials which include: the Assistant Commissioner, Office of Information and Technology, and both Deputy Assistant Commissioners, Office of Information & Technology.
The responsibilities of the AO include the following:

1. Grant the formal security Authorization or Approval-To-Operate (ATO) for a CBP information system.
2. Approve/disapprove system security authorization.
3. Terminate system operation if security conditions warrant such action.
4. Ensure key control compliance is well-documented and annually tested as part of the security authorization of systems supporting: 1) FISMA, 2) Privacy Sensitive Systems, and 3) Chief Financial Officer designated Financial Systems.

5. Require security safeguards, if necessary, greater than the safeguards specified in the security authorization package submitted for approval. This determination will be based on the sensitivity or classification level of the data and the operating environment of an information system.
6. Withdraw security authorization and suspend operations when necessary. Grant waivers to CBP policy when circumstances warrant, and waivers are not in violation of applicable regulations. The AO can grant waivers to CBP policy.
7. Complete the following steps before authorizing an information system that does not include all the security requirements specified in this handbook:
    a. Provide written notification to other Assistant Commissioners owning the data and information system of any security requirements that have not been implemented, residual risks, and mitigating safeguards. Review and approve corrective actions necessary to mitigate residual risk.
    b. Provide the AO and/or an individual with the authority to accept the risk of a non-CBP system connected to a CBP system with a written list of any security requirements that are not implemented, residual risks, and mitigating safeguards.
    c. State in the security authorization document that the Assistant Commissioner, OIT, understands and accepts responsibility for the residual risk, if any, of operating the system.
8. Task the CISO with the development, implementation, and maintenance of an adequate CBP-wide Information Security Program. Within this security program, include the development of procedures necessary to implement applicable security regulations, directives, and publications.
9. Task the Executive Director, Cybersecurity Directorate to formally review and approve all Interconnection Security Agreements (ISAs) that permit the interconnection of CBP-owned systems with any non-CBP-owned systems.
10. Ensure that operational information systems security policies are promulgated for each system for which the Assistant Commissioner and the Deputy Assistant Commissioner, OIT have approval authority.
11. Establish, implement, and maintain an information system security education, training, and awareness program.
12. Report security discrepancies, vulnerabilities, and threats, when applicable, to the non-CBP AO of interconnected systems.
13. Approve incident-reporting procedures.
14. Ensure technically qualified personnel perform security functions.
15. Ensure any individual requiring administrator privileges is reviewed and approved. The AO may delegate this duty to the appropriate system owner or Program Manager.
16. Incorporate security throughout the System Life Cycle (SLC) process.
17. Ensure data ownership is established for each information system, to include accountability and access rights.
18. Review Notices of Findings and Recommendations (NFR) and Plan of Action and Milestones (POA&M).
19. Review and approve corrective actions necessary to mitigate residual risks.

2.5 Chief Financial Officer

The Assistant Commissioner of the Office of Finance is the CFO within CBP. The CBP CFO:

1. Works with the CIO and owners of all designated financial systems to help ensure the reliability of financial data processing through the systems.
2. Develops and establishes policies and procedures regarding automated application controls for software processing of financial data.
3. Remediates automated application controls deficiencies.
4. Works with system owners to designate an Information System Security Officer (ISSO) for each of the designated financial systems as defined in Section 2.9, *Information System Security Officer*.
5. Tracks and monitors progress of automated application controls remediation efforts.
6. Works with system owners of designated financial systems to ensure remediation of Information Technology General Controls (ITGC) deficiencies related to IT policies and procedures.
7. Works with CIO to incorporate user requirements for new financial applications or upgrades to existing financial applications.
8. Works with the CIO to integrate and test CBP-wide business continuity plan.
9. Coordinates with the CIO to identify the financial data needed to be backed up and recovered.

2.6 Chief Information Officer

The Chief Information Officer (CIO) is responsible for overseeing implementation and compliance of CFO-designated financial systems and all other systems. The CIO:

1. Reviews and evaluate the CFO-designated financial systems to ensure ITGCs are in place and working effectively.
2. Works with the system owners to ensure remediation of ITGC deficiencies related to CFO-designated financial systems.
3. Tracks and monitor progress of ITGC POA&Ms and remediation efforts.
4. Ensures completion of Memorandums of Understanding (MOUs) and ISAs for CFO designated financial system interconnections with any system not owned by DHS; ensure that they include appropriate security clauses; and monitor service provider for compliance with MOUs and ISAs.
5. Implements the CBP-wide system development lifecycle methodology and monitor user compliance with this methodology.
6. As part of developing new financial applications or updating existing applications, integrates CFO feedback to ensure user requirement are adequately addressed.
7. Develops and tests CBP-wide disaster recovery plan. Coordinate with the CFO to incorporate business continuity requirements and test on a periodic basis.

8. Based on CFO requirements, executes policies for the routine backing up and recovery of financial data. Implement policies and procedures for rotating back-up media offsite.

2.7 Financial System Owners

Systems owners are responsible for implementing and monitoring CBP policies, processes, and procedures related to the integrity of the data processed through the application and ongoing business processes. They are required to maintain the security of the technical and operational environment hosting the financial applications. Owners of CFO-designated financial systems:

1. Work with the CISO to ensure designated financial systems are properly secured.
2. Designate an ISSO for each of their respective designated financial systems
3. Ensure ITGCs are implemented and tested as required in DHS and CBP policy.
4. Develop, implement, and test application controls, as appropriate.
5. Ensure the completeness, accuracy, validity, and security of data inputs into, processed by, and output from the financial application.
6. Ensure that ISA are completed and enforced.
7. Ensure that system POA&Ms are prepared and implemented with resources identified.
8. Ensure resources are available for correcting weaknesses.
9. Review and update the security of IT systems within their program area, in consultation with the CIO and CISO, at least annually.
10. Prioritize security weaknesses based on material weaknesses, external audits, and program assessments
11. Comply with system development life cycle methodology for new system implementations or modifications to existing systems.
12. Participate in the developing and testing of disaster recovery/IT contingency plans for CFO-designated financial systems.
13. Ensure that security assessments of key security controls (i.e., security control assessments, & Security Assessment Report (SAR)) for CFO Designated Systems are completed annually in the Cybersecurity Assessment and Management (CSAM) system. This includes updating the security control assessment and SAR annually.

2.8 Other Assistant Commissioners

The head of each CBP office shall support the CBP Information Security Program by participation in the activities listed below.

1. Enforce the information systems security policies and procedures set forth in this handbook, including the appointment of the ISSOs in writing, as appropriate, who will report to the CISO.
2. Provide information to the CISO concerning the sensitivity of information under the Executive Assistant Commissioner's purview. This information will assist in the decision regarding the security features that need to be operative, in order to protect the information within the application. This information should be provided during system development and updated whenever there is a change.

2.9 Chief Information Security Officer

The CBP CISO implements and manages all aspects of the CBP Information Security Program to ensure compliance with DHS policy and guidance implementing Federal Information Security Modernization Act of 2014 (FISMA), other laws, and Executive Orders. The CBP CISO reports directly to the CIO on matters relating to the security of CBP Information systems. The CISO provides a SOC that complies with the DHS Security Operations Concept of Operations (CONOPS) (unclassified/classified). The CISO is the Executive Director, Cybersecurity Directorate. Specific duties are detailed below.

Policy ID	CBP Policy Statement	Relevant Controls
2.9.a	CISO develops and maintains a CBP-wide information security program in accordance with the DHS security program.	PL-1
2.9.b	CISO is responsible for overall security management of the CBP enterprise.	---
2.9.c	The CISO serves as the CIO's primary liaison with CBP's information system owners, Program Office Information System Security Managers, and ISSOs.	---
2.9.d	CBP is accountable to the CISO.	---
2.9.e	The CISO implements DHS information security policies, procedures, and control techniques to address all applicable requirements.	PL-1
2.9.f	The CISO develops and manages information security guidance and procedures unique to CBP requirements.	PL-1

CBP CISO

1. Designates (as necessary) one or more subordinate Officials to support national infrastructures. Initiate new security policy change requests as necessary. Issue interim policy in the form of Interim Policy Letters (IPLs). Such letters will be included into *the CBP Information Systems Security Policies and Procedures Handbook* upon its next publication. Develop and publish procedures necessary to implement the requirements of DHS information security policy. Ensure that the security authorization process documentation is recorded in the DHS Security Authorization Process Tool and FISMA Reporting Tool. Serve as the Security Control Assessor for CBP when nobody is officially designated.
2. Ensures all security-related vulnerabilities and incidents are recorded and serious or unresolved security violations are reported to the Assistant Commissioner, Office of Information and Technology (OIT) and DHS.
3. Advises the Assistant Commissioner, OIT of vulnerabilities, residual risks, and use of special security features and mechanisms for each MA and GSS operating on the system. Develop a POA&M to mitigate residual risks.
4. Ensures that rules of behavior and security procedures/guides are developed.

5. Ensures that the results of annual security assessments (e.g., National Institute of Standards and Technology Special Publication (NIST SP 800-53) of MAs or GSSs are properly addressed in funding requests to mitigate identified risks, or carry out the POA&M.
6. Assesses the system during the continuous monitoring phase of the security authorization process, including modifications to the system, its environment, and operational needs that could affect the security posture of the system and its security authorization status.
7. Ensures the appropriate ISSO prepares all ISAs that permit the interconnection of a CBP-owned system with any non-CBP-owned system or external systems. For each ISA submitted for approval, establish proof of adequate information system security measures and recommend approval or disapproval to the signatory authority.
8. Ensures proper protective or corrective measures are taken when an incident or vulnerability is discovered within a system.
9. Approves or disapprove all requests submitted from any source that led to internal or external penetration testing; bypassing, straining or testing security mechanisms; performing target monitoring; keystroke monitoring; or any other functions that may infringe on the performance of either the organization or an individual.
10. Ensure that a security evaluation of the product has been conducted before it is added to the TRM.
11. Serves as a member of the Configuration Management (CM) Board and ensure CM of security-related software and hardware is maintained and documented.
12. Provides oversight of the Continuity of Operations Plans (COOPs) of OIT. Ensure that a contingency plan is prepared and tested annually.
13. All GSSs are under the direct oversight of the CISO, with support from the SOC. All GSSs must have only one ISSO assigned.
14. Designates one or more CBP Information System Security Managers (ISSMs), as necessary, to serve in a supervisory capacity within the program offices and significant and complex IT systems.
15. Each MA must be under the direct oversight of the CISO, with support of the CBP ISSMs and the SOC. All MAs have only one ISSO assigned.

2.10 Information System Security Manager

Through the authority granted by DHS to develop and maintain a Component-wide security program in accordance with the DHS security program, the CISO may designate one or more CBP ISSMs, as necessary, to serve in a supervisory capacity within the program offices and significant and complex IT systems. The ISSM would serve as the coordinator for the CBP information security program within the Program Offices on behalf of the CISO.

As the Security Control Assessor (SCA), the CISO reserves the sole authority to assess IT systems within CBP for the Authorizing Official. Although the ISSM ensures that ISSOs are appointed for each system, the CISO retains veto and approval authority over the hiring or assignment of all ISSOs.

The ISSMs are designated in writing by the CBP CIO, with the concurrence of the DHS CISO.

In addition to abiding by DHS 4300A policy, CBP ISSMs:

1. Ensure that security controls are ALL answered as required by the RTM and address the following four areas: (1) What is the security solution or countermeasure that is in place? (2) Who is responsible for enacting and/or maintaining the solution? (3) How often is the solution implemented/reviewed/updated? (4) How does the identified solution satisfy the requirements of the particular control?
2. Ensure that the Plan of Execution (POE) is determined and approved and then executed as scheduled and agreed upon.
3. Ensure that all policy waiver requests, POA&M extension requests, Memorandums of Understanding (MOUs), and ISAs are reviewed and approved prior to being submitted to the Cybersecurity Directorate for CBP CISO approval.
4. Ensure that all POA&Ms are managed, and all milestones are met.
5. Ensure that all system self-assessments are completed on schedule.
6. Represent security at IT security system audits, critical control or program reviews, and other CBP-level reviews.
7. Ensure that all system connectivity is identified and documented in the security plans and addressed with a MOU and/or ISA as necessary.
8. Work with the STP FISMA Compliance Team to ensure that all FISMA requirements are met and that the FISMA scorecard reflects the goals set by the CBP CISO.

2.11 Security Control Assessor

In addition to abiding by DHS 4300A policy, the CBP Security Control Assessor (SCA):

1. Ensures that the required security authorization process activities are completed, and that the test results are documented.
2. Ensures that a risk analysis is performed and that it identifies risks, determines their magnitude, and identifies areas needing safeguards.
3. Ensures that a system test and evaluation is conducted, and the results of such tests are documented or updated annually.
4. Ensures that rules of behavior and security procedures/guides are developed.
5. Ensures that a contingency plan is prepared and tested annually.
6. Ensures that the security authorization process documentation is recorded in the DHS Security Authorization Process Tool and FISMA Reporting Tool.
7. Reviews the security authorization process package (Security Plan, SAR, and POA&M) and recommends to the AO whether or not the system should be authorized.
8. Prepares the security authorization decision letter for the AO's signature.

2.12 Certification Agent

The Certification Agent (CA) is a technically qualified security professional that reports to the CISO and provides a level of independent evaluation that is required by the security authorization process. The CA provides an independent assessment of the security plan to ensure it provides a set of security controls for the information system that is adequate to meet all applicable security requirements. In addition, the CA is responsible for a comprehensive assessment of the management, operational, and technical controls of the information system to

determine if they are implemented correctly, operating correctly, and meeting the security requirements. The CA recommends corrective actions to reduce or eliminate security vulnerabilities. The results of the assessment of the security controls are documented in the SAR along with a list of recommended corrective actions and a POA&M to ensure implementation. The SAR is the certification agent's statement regarding the security status of 2the information system. The Certification Agent:

1. Assists with information systems security audits and reviews, as appropriate. With the appropriate ISSO, determine the priority level associated with audit findings.
2. Validates that the information system design meets a specified set of managerial, operational, and technical security requirements and that it includes the implementation of an adequate audit trail capability of security-related activities.
3. Determines, with the data owner(s) and ISSO(s), the minimum-security features for each unique application.
4. Ensures security plans are developed for all information systems. Ensure that the application is certified and the certification documentation is developed using the DHS security authorization process tool, CSAM.
5. Reviews and evaluates security impact of changes to the applicable IT system, including interfaces with other networks.
6. Observes the testing of security controls for assigned MAs and GSSs.
7. Provides written justification, when appropriate, to the CISO for approval by the Assistant Commissioner, OIT to obtain a written waiver of or exception to the policy for mandated security features.
8. Reviews Security Authorization Packages and work with the assigned ISSOs and system owner to ensure that the security requirements of the system have been documented, tested, and implemented. Write the SAR and include the Certification Statement as part of the SAR. The final POA&M and a list of residual risks must also be included in the Security Authorization Package. Forward the Security Authorization Package to the CISO and AO for approval.
9. Represents STP at key project meetings, as directed by the CISO.
10. Validates CSMA submissions for FISMA compliance.
11. Maintains an on-line copy of the following documents and ensure the documents are current: annual security self-assessment (i.e., NIST SP 800-53), SAR, Security Plan (SP), Security Risk Assessment Report, Contingency Plan and Test Results, Security Test Plan and Evaluation, Vulnerability Scan Results, signed POA&M, and Signed Security Authorization Transmittal Letter.

2.13 Information System Security Officer

In CBP, ISSOs are responsible for ensuring the implementation and effectiveness of security controls in accordance with Department policies. The ISSOs ensure a system is adequately protected while also addressing the legitimate needs of the user community for access and availability. System Owners/Managers will provide the majority of ISSOs and the CISO will

appoint all ISSOs in writing using the *Information Systems Security Officer (ISSO) Designation Letter.*

Policy ID	CBP Policy Statement	Relevant Controls
2.13.a	An ISSO may be assigned to more than one system, but a system may only be assigned one ISSO. Multiple Alternate (AISSOs) may be designated to assist the ISSO.	PL-1

Specific ISSO duties are detailed below.

1. Ensure that systems are operated, maintained, and disposed of in accordance with internal CBP security policies, practices, and procedures outlined in this handbook.
2. Determine the appropriate levels of security required to protect integrity, availability, and confidentiality of the information system data, and verify these levels with the CA and/or CISO.
3. Conduct an information system security analysis to determine and document appropriate security requirements during the design stage of an application.
4. Assist developers to incorporate security requirements into their applications that comply with all laws, regulations, and security policies. Verify that these requirements are appropriate, sufficient, and comply with organizational infrastructure standards.
5. Develop and maintain all Security Authorization Packages generated for assigned systems and coordinate each security authorization package with the appropriate personnel.
6. Develop and maintain all ISAs that permit the interconnection of CBP-owned systems with any non-CBP owned systems.
7. Ensure all security related incidents are immediately reported to the CBP SOC in accordance with the CBP incident response policy and DHS 4300A Attachment F *Incident Response.*
8. Initiate protective or corrective measures when a security incident or vulnerability is discovered.
9. Ensure security features are properly restored and procedures are followed during system recovery processes.
10. Ensure all information system security-related documentation is current and accessible to authorized individuals.
11. Ensure a virus-free environment by coordinating with systems operations to maintain current anti-virus engines and signature files on all workstations and servers.
12. Ensure that requests to bypass, strain, or test security mechanisms are forwarded in advance to the CISO for review and approval.
13. Certify that appropriate procedures are used to cleanse system components before they are released (See Section *Media Controls*).
14. Notify the responsible CA and CISO when changes occur that might affect security authorization. This includes the recommendation to rescind any security authorization when systems are no longer used or fail to maintain the required security posture.

15. Inspect information systems to ensure the absence of unapproved software (including shareware and copyrighted software) and ensure the presence of the approved Department Security Warning Banner.
16. Ensure that security training programs applicable to all assigned security personnel are developed and maintained for applications and systems assigned to them.
17. Using SOC audit tools, ensure that audit logs for assigned systems are reviewed for security anomalies.
18. Develop a test plan and test the security controls that have been developed for assigned information systems. The CA should also observe the testing of the security controls.
19. Provide system owners and developers with appropriate budgetary inputs to ensure that information security features and operations are adequately funded. Assist system owners and developers to ensure that results of periodic security self-assessments, risk assessments, and independent audits are reflected in subsequent program funding requests.
20. Maintain a file of the following documents and ensure the documents are current:
    a. Copies of all security authorization packages developed for assigned systems.
    b. Copies of all security policy documents.
    c. Copies of security risk assessments performed on assigned applications and/or information systems including vulnerability assessments for the same.
    d. A copy of the last information system Security Self-Assessment or NIST SP 800-53 for each assigned MA or GSS.
21. Serve as a liaison between system owners and the CISO.
22. Work with system owners to document weaknesses in POA&Ms and initiate corrective action.

ISSOs Supporting Privacy Sensitive System:

1. Update Security Plans documenting the implementation of all key Privacy controls.
2. Update risk assessments to address risks associated with Data Transport and Off-site storage, Remote Access to Personally Identifiable Information (PII) Data and Remote Storage.
3. Monitor key operational Privacy Controls to ensure controls remain in compliance.
4. Verify erasure of any expired PII extracts.
5. Obtain System Owner and CBP Privacy Officer's approvals to extract PII computer-readable data extracts that are outside of a security plan.
6. Perform or oversee performance of day-to-day security operations of the system.
7. Develop or assist in development of the system security policy.
8. Ensure compliance with system security policy.
9. Assess security impact of system changes.
10. Develop and update the security plan.

ISSOs Supporting CFO-Designated Financial Systems:

1. Update Security Plans documenting the implementation of all key financial and financial internal controls.

2. Update Risk Assessments to address risks and potential impacts to the financial statement associated with security control weaknesses.
3. Monitor key operational Financial Controls to ensure controls remain in compliance.
4. Perform annual NIST SP 800-53 assessments for all required controls (100% coverage).
5. Provide support to annual financial systems audits as directed by the system owners and the CISO.

2.14 Supervisors and Managers

Supervisors and managers are responsible for maintaining information system security within their specific work environments. The responsibilities of supervisors and managers include the following:

1. Protect sensitive information system data and resources within their area of responsibility with appropriate security safeguards.
2. Verify that subordinates have access to only those information system applications and data necessary to perform authorized tasks (principle of least privilege). DO NOT authorize more than one account on the same system for an individual.
3. Conduct an annual review of current access lists for each system accessed by subordinates and revalidate their access requirements.
4. Ensure that proposed acquisitions of information system-related hardware, software, communications, applications, and equipment satisfy information system security requirements, meet security Technical Reference Model (TRM) architecture standards, and receive ISSO concurrence before acquisition. As part of the investment management program (See Section 3.2, Capital Planning and Investment Control), security requirements must be developed and funded in accordance with the Office of Management and Budget (OMB) budget request guidelines.
5. Ensure that subordinates receive information system security training relevant to their assignments, as required by law, regulations, Memorandums of Understanding (MOUs) or other agreements.
6. Attend information system security training as required by law, regulations, MOUs, or other agreements.
    a. Execute limited personal use policy for CBP employees and vendor support personnel using CBP-owned office equipment in accordance described in DHS MD 4600.1, *Personal Use of Government Office Equipment*, and DHS MD 4900, *Individual Use and Operation of DHS Information Systems/Computers*.
    b. Obtain, review, and enforce compliance with the "Limited Personal Use Policy" stated within the directive.
    c. Review and approve/disapprove each employee's request for personal use of CBP-owned systems. If there are any questions, contact the CISO.
    d. Respond to employee questions regarding acceptable use of government office equipment for personal reasons.

e. Once approved, determine employee need for personal use annually, monitor for inappropriate usage, and reinforce this policy to restrict, suspend, or refuse the privilege of personal use when appropriate. Notify the CISO of violations of this policy.
f. Revoke or limit the privilege to use such equipment for non-government purposes as necessary. All revocations will be reported as a security incident.

2.15 Privacy Officer

The CBP Privacy Officer will be assisted by the DHS Chief Privacy Officer (CPO) to comply with Federal laws and DHS privacy policy. The CBP Privacy Office will work with the CIO and DHS CPO to maintain privacy requirements. The CBP SOC shall work with the CBP Privacy Office or with the DHS CPO to address suspected or confirmed Privacy Incidents (PI) or incidents involving PII.

The CBP Privacy Office is responsible for:

1. Advise the CIO and management regarding privacy issues.
2. Review PTAs prior to submission to the DHS CPO for accuracy, and provide any additional information needed after submission to assist the DHS CPO with a determination as to whether it is a privacy sensitive system.
3. Work with system owners who maintain privacy sensitive systems to complete required PIAs and SORNs and review documentation for mitigating possible privacy risks.
4. Coordinate with program managers, CISO, SOC in evaluating and reporting suspected or confirmed privacy incidents.
5. Implement the Privacy Incident Response Plan as outlined in the DHS Privacy Incident Handling Guidance (PIHG).
6. Periodically review logs maintained by system owners, program managers, or supervisors for computer-readable PII data extracts not covered by a security plan.
7. Implement Privacy Awareness training and education as directed by the DHS CPO.

2.16 Program Managers

In addition to responsibilities outlined in DHS4300A, CBP Program Managers shall:

1. Work with system owners, CISO, and their staffs to ensure information systems are properly secured.
2. Understand how to recognize and respond to suspected or confirmed security incidents, privacy incidents or incidents involving PII.
3. Consult with the privacy office concerning privacy incidents and other privacy issues affecting IT systems and programs under his or her control.
4. Prepare and transmit written Privacy Event Notification (PEN) simultaneously to the privacy office, CIO, and CISO.
5. Supplement privacy incident reports to the SOC and CISA as information becomes available.

6. Prepare and submit to the Privacy Office for approval of PTA for systems or programs, and PIAs and SORNs, as required and provide additional information to the Privacy Officer to finalize the required documents. In some instances, changes to the system or the standard operating procedures may be required to reduce the impact on privacy and receive approval of the program from the DHS Chief Privacy Officer.
7. Develop standard operating procedures to handle routine computer-readable PII data extracts that are removed from the system security boundaries of the Security Plan of the security authorized system. Computer-readable PII data extracts that are not covered by an appropriate SP must be logged and may be reviewed periodically by the DHS Privacy Office or the Privacy Officer for compliance.

2.17 Information System Owners and Information Owners

In the context of this handbook, system owners and information owners are responsible for categorizing the security of data and/or systems in accordance with Federal Information Processing Standards Publication (FIPS PUB-199), in addition to other role-based responsibilities. The distinction between system owners and information owners is not immediately obvious, and the roles may fall to different individuals, depending on the life cycle of the system. A single information system may process data from multiple information owners. Likewise, an information owner's data may reside on or be processed across multiple information systems. The information owner is responsible for ensuring the integrity and confidentiality of the information/data.

In the CBP environment, for example, an organization that owns development of a new application must coordinate with information owners to define the security categorization and requirements of the data processed by the application. In the production environment, system owners must identify and maintain the security level of the servers, Local Area Network (LAN), and other devices, which support operation of one or many applications.

In addition, system owners and information owners shall:

1. Ensure that a final security authorization package is signed by the AO before the system is implemented in production.
2. Ensure that an ISSO is formally assigned to each IT system under their control and that this assignment is appropriately documented.
3. Ensure that required computer security functions and documentation are included in system life cycle planning and budgets and appropriate resources are available for the security authorization.
4. Work closely with the CIO and other program and IT managers to ensure a complete understanding of risks, especially the increased risks resulting from interconnectivity with other programs and systems.
5. Document and manage accepted security risks in risk assessments.

6. Prioritize security weaknesses for mitigation based on material weaknesses, external audits and program assessments and ensure mitigation funding is made available or requested.
7. Ensure that all reported security-related incidents are immediately reported to the CBP SOC in accordance with DHS 4300A Attachment F *Incident Response*. Investigate security incidents to support the SOC, if directed.
8. Develop PIAs and obtain PIA approvals from the DHS Privacy Office for privacy systems.
9. Ensure necessary resources are allocated to remediate any areas of privacy sensitive systems that are non-compliant with key privacy controls.
10. Provide necessary system-related documentation to the certification agent.
11. Take appropriate steps to reduce or eliminate system vulnerabilities identified in the security authorization process.

2.18 System and Network Administrators

System Administrators (SAs) and Network Administrators are responsible for daily operation and maintenance of systems. SAs keep systems and LANs operating and in service for the users. Where information security is concerned, any resource that performs the duties of an SA has the following responsibilities:

1. SAs, who have a need for and have been granted root access, are responsible for protecting the root, administrator or super user authenticator at the highest sensitivity level it secures. These SAs should not share the authenticator and/or account.
2. Report all suspected information system security-related problems, security anomalies, system vulnerabilities or suspicious activities of authorized users to the ISSO assigned to the system.
3. Notify the ISSO and the change control board of any major system changes or system configuration changes that might adversely affect systems security.
4. Use special access or privileges granted to perform only authorized tasks and functions.
5. Notify the SOC of any detected violations of user access to assure timely detection of suspicious, inappropriate, or unauthorized activity.
6. Establish audit trails and facilitate their review when required.
7. Maintain configuration control of the system and its application software.
8. Notify the ISSO when feasible security safeguards and features are not implemented on the information system or network.
9. Do not attempt to strain or test security mechanisms without authorization from the CISO or perform target or keystroke monitoring of an individual without written authorization from the Office of Professional Responsibility (OPR). Request permission for such testing or monitoring through the ISSO.
10. Participate in computer security incident reporting in accordance with DHS 4300A Attachment F *Incident Response.*

11. Support compliance with functional security requirements as requested by the ISSO for locally developed, sensitive information system products, as appropriate.

2.19 System Control Officer

A System Control Officer (SCO) has the following responsibilities:

1. Revoking or suspending application access when a user separates from CBP or is transferred.
2. Documenting and retaining the authorization in accordance with procedures identified for each system.
3. Providing the ISSO and auditors with authorization documentation when requested.
4. Reporting user provisioning issues to the ISSO or a SCO chain ending with the National SCO as needed.

SCOs shall not grant or revoke system access or privileges to individuals without written authorization. To do so is a security violation and it may result in disciplinary action.

3.0 Management Policies

Basic security management principles must be followed to ensure the security of Department of Homeland Security (DHS) information resources. Management controls consist of techniques and concerns that are normally addressed by management personnel as indicated in the following sections.

3.1 Capital Planning and Investment Control

DHS Management Directive (MD) 102-01 Rev. 2, Acquisition Management Directive and DHS MD 4200.1, IT Capital Planning and Investment Control (CPIC) and Portfolio Management provide the foundation on these requirements. The following are CBP-specific policies:

Policy ID	CBP Policy Statement	Relevant Controls
3.1.a	CBP ensures that information security requirements as described within this Policy Directive are met in the acquisition of all DHS information systems and services used to input, process, store, display, or transmit sensitive information.	SA-1
3.1.b	CBP procurement authorities ensure that the Department of Homeland Security Acquisition Regulation (HSAR) provisions are fully enforced.	SA-1

CPIC responsibilities include:

CBP CIO:

- Coordinates the review of an independent evaluation of the DHS annual budget submission to ensure that information security requirements are adequately addressed.
- Coordinate and advocate resources for Identification and Authentication (IA) enterprise solutions.

- Ensure that funding for implementation of information security is included in project life cycle planning.

CISO:

- Ensure that information security requirements are included in the organization's capital planning and investment management planning processes.

System Owner:

- Ensure that funding for implementation of information security is included in project lifecycle planning.

3.2 Contractors and Outsourced Operations

Computer security requirements must be incorporated in contractual documents involving the acquisition, development, and/or operations and maintenance of computer resources. This applies at the beginning of a project or acquisition and in all follow-on contracts or purchasing agreements involving the acquisition of computer resources. This includes hardware, software, maintenance, and other associated IT products and services.

Policy ID	CBP Policy Statement	Relevant Controls
3.2.a	All Statements of Work (SOW) and contract vehicles identify and document the specific security requirements for IT services and operations required of the contractor.	SA-1
3.2.b	Contractor information system services and operations adhere to all applicable CBP and DHS information security policies.	SA-1
3.2.c	Requirements address how sensitive information is to be handled and protected at the contractor's site, including any information stored, processed, or transmitted using the contractor information systems. Requirements also include requirements for personnel background investigations and clearances, and facility security.	SA-2 SA-5 SA-9 (5)
3.2.d	SOWs and contracts require that at the end of the contract, the contractor must return all information and information resources provided during the life of the contract and certify that all CBP information has been purged from any contractor-owned system(s) that have been used to process CBP information.	MP-4
3.2.e	CSD conducts reviews to ensure that the information security requirements and provisions to address supply chain risk are included within the contract language and provisions are met throughout the life of the contract.	SA-1
3.2.f	Security deficiencies in any outsourced operation require creation of a program-level POA&M.	SA-9
3.2.g	CBP require contractors to apply information system security engineering principles in the specification, design, development, implementation, and modification of information systems, in	SA-8

	accordance with NIST SP 800-27, *Engineering Principles for Information Technology Security.*	
3.2.h	For systems with high or moderate impact for any of the FIPS 199 security objectives, CBP require developers of an information system, system components, or information system services to: a. Perform CM during system, system component, or service development and implementation b. Document, manage, and control the integrity of changes to items under CM c. Implement only organization-approved changes to the system, system component, or service d. Document approved changes to the system, system component, or service and the potential security impacts of such changes e. Track security flaws and flaw resolution within the system, system component, or service and report findings to the DHS ESOC.	SA-8
3.2.i	For systems with high or moderate impact for any of the FIPS 199 security objectives, CBP requires developer of information systems, system components, or information system services to: a. Create and implement a security assessment plan b. Perform: unit; integration; system; regression testing/evaluation commensurate with the volume and complexity of modifications and the impact to the system risk made by those modifications c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation d. Implement a verifiable flaw remediation process e. Correct flaws identified during security testing/evaluation.	SA-11
3.2.j	All SOW, contract vehicles, and other acquisition-related documents include privacy requirements and establish privacy roles, responsibilities, and access requirements for contractors and service providers.	
3.2.k	CBP Procurement authorities ensure that HSAR provisions are fully enforced.	SA-1
3.2.l	All companies providing services to CBP are required to comply with the CBP *Information Systems Security Policies and Procedures Handbook*.	SA-9
3.2.m	All support staff are trained in basic network, hardware, and security principles of CBP.	PS-2
3.2.n	All CBP employees and contractors are U.S. citizens and have a favorably adjudicated Background Investigation (BI) completed.	PS-3

Responsibilities for contractors and outsourced operations include:

CISO

- Establish and maintain a contractor and outsourced operations policy for CBP.

System Owner/IT Project Manager

- System Owners and Project Managers must review and include security requirements in solicitation documents *prior to the acquisition of information systems or services*.
- Ensure that computer security requirements are reviewed and included in all applicable statements of work and other contractual agreements throughout the SELC.
- Ensure that basic security requirements are integrated into the software and procurement life cycle for project development.
- Ensure that computer security requirements are specified in the system design and functional requirements documents, and other SELC documents, as required.

ISSO

- Coordinate with the system owners to ensure that contractor and outsourced operations policy requirements are met.

3.3 System Engineering Life Cycle

The DHS Systems Engineering Life Cycle (SELC) is detailed in Acquisition Management Directive 102-01 Rev.2, Appendix B. Additional CBP policies include:

Policy ID	CBP Policy Statement	Relevant Controls
3.3.a	Ensure that system security is integrated into all phases of the SELC.	SA-3
3.2.b	Ensure that security requirements for sensitive information systems are incorporated into system life-cycle documentation.	SA-3
3.2.c	System owners ensure that adequate funding is available for implementation of security requirements.	SA-

3.4 Configuration Management

The Office of Information Technology (OIT) configuration management program is an important component of our security program. The CM discipline applies to hardware, including power systems, software, firmware, documentation, test and support equipment, and spares. The DHS 4300A Attachment CC includes the NIST 800-53 rev. 5 Baseline Controls.

3.5 Security Authorization and Security Control Assessments

Federal Information Security Modernization Act of 2014 (FISMA) directs that all Federal agencies develop and implement a Department-wide Information Security Program designed to safeguard IT assets and data. CBP bases its Security Authorization policy on DHS policy and the recommendations set forth in NIST SP 800-37, Rev. 2 and OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources.

It is recommended that CBP pursues Type Security Authorization for information resources that are under the same direct management control; have the same function or mission objective, operating characteristics, security needs, and that reside in the same general operating environment, or in the case of a distributed system, reside in various locations with similar operating environments.

Type Security Authorization shall consist of a master security authorization package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites.
The DHS *Security Authorization Process Guide* describes detailed processes governing security authorizations.
Detailed information for creating and managing POA&Ms is published in DHS 4300, Attachment H*, – Plan of Action and Milestones (POA&M) Process Guide*.

Security Control Assessment is the comprehensive testing and evaluation of the management, operational, and technical security features of an IT system. It primarily addresses software and hardware security safeguards; considers procedural, physical, and personnel security measures; and establishes the extent to which a particular design and implementation meets a specified set of security requirements. It also considers procedural, physical, and personnel security measures employed to enforce information security policy.

Security Authorization is the official management decision by the AO, which authorizes the operation of a system. It includes explicitly accepting the risk to Department operations, assets, or individuals, based on the implementation of an agreed-upon set of security controls. The AO accepts security responsibility for the operation of certified IT systems and officially grants that a specified IT system is ATO based on these protections. The AO shall be identified in IACS. The CBP CIO will serve as the AO for any system where an AO has not been appointed or where a vacancy exists.

A common controls approach (type authorization) may be used for authorizing systems. Attachment D to this Handbook, “Type Authorization,” provides specific guidance. The AO must approve the use of any common controls-based Security Authorization Process.
CBP categorize systems in accordance with FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems” and apply the appropriate NIST SP 800-53 and NIST 800-161 controls. The IACS automated tool is used to produce Security Authorization Process packages. IACS supports the POA&M process, quarterly reports and annual self-assessments.

The DHS Security Authorization Process Guide provides detailed instructions for creating authorization artifacts, using authorization tools for authorizing systems, and the timeline for creating authorization artifacts, tracking remediation activities, and performing the required self-assessments and generating the required reports.

Required Security Authorization Processes to be completed for sensitive systems are detailed in

DHS 4300A. Sensitive Compartmented Information (SCI) Systems are authorized by the DHS Office of Intelligence and Analysis (DHS I&A).

All production IT systems (Major Applications (MA), General Support Systems (GSS)) are to undergo security authorization. In some situations, a common controls (type security authorization) approach may be used for authorizing a system as defined by CBP, DHS, and NIST guidance. Prior to starting a common controls-based security authorization, agreement should be reached with the AO to ensure a sufficient approach is performed. See Appendix D, Type Accreditation for more information on type certification/security authorization.

In accordance with approved DHS information security policy, the CSAM tool shall be used to produce security authorization packages for all IT systems. All IT systems shall be authorized using CSAM. The NIST 800-53 controls must be applied. Applying the NIST 800-53 controls requires that systems be categorized.

Artifacts generated during the security authorization process are uploaded into CSAM, which supports the remediation process with its capability to manage the POA&M process and which generates quarterly reports and the required annual self-assessment.
The artifacts required are listed below:
1. FIPS 199 Categorization
2. Privacy Impact Assessment (PIA)
3. E-Authentication
4. Risk Assessment
5. Security Plan
6. Contingency Plan
7. Security Control Assessment
8. Contingency Plan Testing
9. SAR
10. ATO—includes updated Security Plan, POA&M, and SAR
11. Annual NIST SP 800-53-based self-assessments

Policy ID	CBP Policy Statement	Relevant Controls
3.5.a	CBP will use DHS approved and specified tools, techniques, and methodologies to assess and authorize DHS information systems, report and manage FISMA data, and document and maintain POA&Ms.	CA-1
3.5.b	Currently all CBP systems are authorized using the DHS CISO approved automated tool, CSAM.	CA-1 CA-2
3.5.c	All security authorizations for unclassified and collateral classified systems will be done following DHS 4300A policies and procedures, in addition to CBP Security Authorization process. SCI Systems are authorized following the process approved by the DHS Office of Intelligence and Analysis (DHS I&A).	CA-1

3.5.d	DHS CISO maintains a repository for all Security Authorization process documentation and modifications.	CA-1
3.5.e	CBP CISO establishes processes to ensure consistent Security Authorization processing across all CBP IT systems.	CA-1

Assessment and Authorization responsibilities:

Security Control Assessor

- Ensures that the SP, Security Control Assessment, Contingency Plan, and Risk Assessment contain the information required for the Security Authorization Process
- Prepares the assessor's statement, which reflects the state of the security controls, based on the results of the Security Control Assessment
- Recommends to the AO the possible implementation of additional risk mitigation actions that would mitigate the residual risks identified by the Security Control Assessment
- Assembles the assessment package that includes the assessment findings, and transmit to the AO
- Maintains files of assessment packages for each system

System Owner

- Ensure that adequate resources are budgeted for and allocated to the Security Authorization process.
- Review the results of the Initiation and Security Certification phases and ensure resources are provided to identify and implement risk mitigation measures.

Certification Agent

- Participate in the early phase to assist the development team in identifying specific security requirements.
- Validate the security design decisions of the development teams and the ISSOs.
- Determine with the data owner(s) and ISSO(s), the minimum-security features for each unique application.
- Observe the testing of security controls for assigned MAs and GSSs.
- Ensure that the Security Plan, Security Control Assessment, Contingency Plan, and Risk Assessment contain the information required for Security Authorization.
- Ensure security plans are developed for all information systems. Ensure that the system is certified, and the certification documentation is developed using the DHS Security Authorization tool.
- Review the security documentation.
- Write the SAR and include the POA&M and a list of residual risks.
- Write the Certification Statement, which reflects the state of the security controls, based on the results of the Security Control Assessment, and review Security Authorization Package and recommend approval to the Security Control Assessor.

3.6 Privacy Sensitive Systems

Refer to the following documents for additional information and policies on protecting PII and Sensitive PII at DHS:

- *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security*
- DHS 4300A, Attachment S, *Compliance Framework for Privacy Sensitive Systems*
- DHS 4300A, Attachment T, *Managing Computer-Readable Extracts Containing Sensitive PII*

Policy ID	CBP Policy Statement	Relevant Controls
3.6.2.e	For Privacy Sensitive Systems, the confidentiality security objective is assigned an impact level of moderate or higher.	---

3.7 E-Authentication

Identity verification or authentication (e-authentication) is needed to ensure that online Government services are secure and individual privacy is protected. Each DHS/CBP system must be evaluated to determine as to whether e-authentication requirements apply.

Policy ID	CBP Policy Statement	Relevant Controls
3.7.a	For systems that allow online transactions, Components determine whether e-authentication requirements apply. For purchases or fee transactions using credit cards, Components comply with Payment Card Industry Data Security Standard (PCI DSS).	IA-2

3.8 CFO Designated Financial Systems

DHS CFO designated systems are systems that require additional management accountability and ensure effective internal control exists over financial reporting. This section provides additional requirements for these systems based on Appendix A to OMB Circular A-123, *Management's Responsibility for Internal Control*. Controls required to be assessed annually for CFO designated systems may be found documented in 4300A Attachment R, *Compliance Framework for CFO- Designated Financial Systems.*

Policy ID	CBP Policy Statement	Relevant Controls
3.8.a	The CISO ensures that incidents related to their respective CFO designated systems are reported to the CBP CFO.	IR-4 IR-6
3.8.b	The SP is updated for CFO designated systems at least annually. Key controls prescribed in *Attachment R, Compliance Framework*	PL-2

	for CFO designated systems are identified in the SP.	
3.8.c	The CISO requests a waiver from the DHS CISO if a key control weakness is identified for a CFO designated system and not remediated within 12 months.	CA-5 CA-7
3.8.d	CFO ensures that a full-time dedicated ISSO is assigned to each CFO designated system. ISSOs should not be assigned collateral duties outside information security responsibilities. CFO Designated system ISSOs may be assigned to more than one CFO designated system.	---
3.8.e	CFO designated system ATO are rescinded if CBP fails to comply with testing and reporting requirements established within this policy.	CA-1 CA-6
3.8.f	CBP CFO works with the CISO to approve any major system change to CFO designated system identified in the DHS inventory.	CA-1 CM-8
3.8.g	CBP CFO ensures that supply chain risk is identified and evaluated prior to all contract awards, changes, and whenever supply chain threat information indicates the existence of unmitigated system, program, or mission risk.	---
3.8.h	System owners are responsible for ensuring that risk assessments for all CFO designated financial systems are updated at least annually.	---

4.0 Operational Controls

Operational Controls address security methods executed by users of information systems, which may include a business process owner, administrator, and users of information systems. These controls are put into place to improve the security of a group, particular system, or a group of systems by requiring a standard of care. This section describes operational controls required in CBP.

4.1 Personnel

4.1.1 Citizenship, Personnel Screening, and Position Categorization

All personnel accessing CBP systems are required to have an appropriate security clearance; a favorably adjudicated background investigation commensurate with the defined sensitivity level of the positions they hold; and a valid need to know. The appropriate position sensitivity level is based on such factors as the type and degree of harm the individual can cause through misuse of the computer system (e.g., disclosure of sensitive information, interruption of critical processing, computer fraud).

Another prudent safeguard is to ensure that individuals who support CBP systems are highly qualified technically and are adequately trained for the position they occupy. This can reduce the risk of unintentional actions. A major threat to an IT system can be the loss of key technical personnel. While unintentional acts and accidents cannot be eliminated, effective training can help to mitigate the possibility or frequency of unintentional user errors.

Sensitivity levels for all Government positions involving the use, development, operation, or maintenance of information systems are required to be designated, and risk levels for contractor positions are required to be determined. See CBP Office of Professional Responsibility's 1400-07A Personnel Security Handbook for details concerning background investigations.

Policy ID	CBP Policy Statement	Relevant Controls
4.1.1.a	CBP ensures incumbents in positions hat use, develop, operate, or maintain information systems have favorably adjudicated background investigations commensurate with the defined position sensitivity levels. As defined in the Office of Professional Responsibility (OPR) 1400-07A, all applicants for a position with CBP must undergo an investigation to determine suitability for employment. Based on the position sensitivity designation, OPR's Personnel Security Division (PSD) initiates either an Office of Personnel Management (OPM) Tier 4 or OPM Tier 5 BI.	PS-1 PS-2
4.1.1.b	Personnel, who have favorably completed initial checks are permitted access to Local Area Networks (LANs), printers, electronic messaging, CBP Intranet and the Internet. However, the individual does not have full computer access until the investigation has been conducted and adjudicated. Access is allowed to any For Official Use Only (FOUO) data, but not Law Enforcement Sensitive documents or data.	PS-3
4.1.1.c	CBP ensures that only U.S. Citizens are granted access to DHS/CBP systems and networks. Exceptions to the U.S. Citizenship requirement may be requested by submitting a completed Foreign National Access Request form for each foreign national to the CBP Foreign Access Coordinator at FSNREQUESTS@CBP.DHS.GOV. See Attachment A- *Foreign Service Nationals* for more details.	PS-2
4.1.1.d	With the consent of the business owner, access to certain administrative systems and shared drives is available to personnel who have successfully completed the initial BI checks as part of the BI process and who also possess written approval of their direct supervisor.	PS-3 AC-1
4.1.1.e	Non-CBP personnel who access CBP information systems and data (e.g., members of the trade community, local law enforcement, Department of State Foreign Service National (FSN)/Locally Employed Staff (LES), or emergency response personnel) are identified. Access will be authorized through procedures that comply with CBP system access policies.	AC-1 PS-3(3)

4.1.1.f	Non-CBP technical support personnel who are required to perform maintenance on CBP information systems within CBP-controlled facilities are escorted at all times, unless they have been approved for unescorted access after having completed a BI.	MA-5
4.1.1.g	Verify that non-U.S. citizens do not perform maintenance.	---

4.1.2 Segregation of Duties

Segregation of Duties (SOD) divides the steps in a critical function among different individuals. OMB Circular A-123, "Management Accountability and Control," requires that key duties and responsibilities in authorizing, processing, recording, and reviewing official agency transactions be separated among individuals. Managers should ensure that individuals do not exceed or abuse their assigned authority. Segregation of duties is intended to prevent a single individual from being able to disrupt or corrupt a critical security process.

Segregation of duties is necessary for adequate internal control of sensitive systems, because it ensures that no single individual has total control of a system's security mechanisms, and prevents a single individual from acting alone to subvert a critical process or otherwise compromise the system.

Assignment and segregation of system responsibilities must be clearly defined and documented for all DHS systems. Segregation of responsibilities, in addition to appropriate access controls, is intended to ensure that no individual has all necessary authority or information access needed to engage in fraudulent activity without collusion. It is essential that thorough and specific job descriptions be documented for every individual working with DHS systems and sensitive information.

An example of segregation of duties is the segregation of security duties on a network system. One individual would be responsible for backing up the system; another responsible for the physical access controls; and another responsible for the access privileges.

Whenever practical, the positions of security administrator and system administrator should be assigned to different individuals. The same principle should be applied to ISSO and system administrator positions. When it is not possible to have separate system and security administrators, the system administrator is responsible for maintaining the system security configuration, and is subject to periodic audit/configuration review by the ISSO.

If CBP does not have sufficient manpower resources necessary to meet strict segregation of duties requirements, the appropriate Authorizing Official (AO) may authorize exceptions, provided that a shortage of personnel is formally identified as a residual risk and compensating controls have been established.

Because SOD is so critical, it is important to define "Sensitive Functions" and "Sensitive Transactions" as it relates to SOD risks. As a minimum baseline, Sensitive functions include a variety of technical functions and activities (i.e., Role-based, Activity based, etc.), business

application functions and operational procedures that present a high impact to CIA of critical data assets through error, fraud, and/or material misstatement. Sensitive transaction is a business transaction that has the potential to negatively impact the organization's financial statements through fraud, material misstatement or financial manipulation by comingling custody of assets, record keeping, and authorization or reconciliation business/application activities. Each of these guidelines should lead to formally defining and documenting at the IT system level. They should also be used as a filter when determining any SOD risks.

Policy ID	CBP Policy Statement	Relevant Controls
4.1.2.a	CBP divides and separate duties and responsibilities of critical information system functions among different individuals to minimize the possibility that any one individual would have the necessary authority, or systems access to be able to engage in fraudulent or criminal activity.	AC-2 AC-5
4.1.2.b	All individuals requiring administrator privileges are reviewed and approved by the appropriate AO. The AO may delegate this duty to the appropriate System Owner or Program Manager.	AC-2
4.1.2.c	Administrator accounts are used only for performing required administrator duties. All other functions not directly tied to administrator duties (checking email, accessing the Internet, etc.) are performed through individuals' regular user accounts.	AC-6
4.1.2.d	Compensating security controls are placed on all Sensitive Functions and Sensitive Transactions to ensure proper management.	---

4.1.3 Information Security and Privacy Awareness Training

In addition to the training requirements outlined in DHS 4300A, the following are CBP Contracting Officer Representative (COR) Responsibilities:

- Ensure that contractors have their personnel complete an initial security awareness course as part of their orientation.
- Ensure that contractors have their personnel complete an annual refresher security awareness course.
- Ensure that contractors have their personnel sign the appropriate Rules of Behavior for use of systems and applications prior to receiving access.
- Ensure that contractors provide additional security awareness training to their personnel whenever there is a significant change in the system security environment or in procedures, or when contractor personnel enter a new position.
- Ensure that contractors maintain a training record for their personnel who have completed initial and refresher security awareness training; ensure that the record includes the name of the person trained, the type and date of the training, and training cost.

4.2 Personal Use of Government Equipment and DHS/CBP Systems

This section discusses CBP policies applicable to the personal use of Government office equipment and CBP IT systems/computers. Policies governing personal use are derived from several DHS Management Directives and CBP Directive 5230-031A

The use of Government-furnished property, including but not limited to office equipment, supplies, computer equipment, software, telecommunications devices, networks, and IT systems, is for official, authorized purposes only. Some limited personal use is allowed, but only when such use:

- Involves minimal additional expense to the Government
- Takes place during the employee's non-work time (i.e., time when the employee is not expected to be addressing official business)
- Does not reduce productivity or interfere with the mission or operations of CBP
- Does not violate the Standards of Ethical Conduct for Employees of the Executive Branch
- Does not allow for intermingling of government and personally owned computing systems. Employees are permitted to use a government system in its standard configuration only.

In addition, any limited personal use must be appropriate. Examples of inappropriate use include the following:

- Use of Internet sites resulting in an additional charge to the Government.
- Creating, downloading, obtaining, viewing, storing, copying, or transmitting sexually explicit or sexually oriented materials, materials related to illegal gambling, illegal weapons, terrorist activities, or any other illegal or prohibited activities.
- Use of government office equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public (e.g., hate speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation).
- Use for other than official Governmental business that result in significant strain on CBP's computer systems (e.g., mass mailings or sending or downloading large files such as programs, pictures, video files, or games).
- Any otherwise prohibited activity, such as sending out solicitations or engaging in political activity prohibited by the Hatch Act.
- Engage in any outside fund-raising activity, endorsing any product or service or participating in any lobbying activity.
- Modifying equipment, including loading personal software or making configuration changes to accommodate personal use.
- Use of government systems as a staging ground or platform to gain unauthorized access to other systems.

- The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.
- Use of CBP systems for commercial purposes, in support of "for-profit" activities, or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services).
- Use of CBP systems for posting agency information to external newsgroups, bulletin boards, or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a government employee or representing the government as a vendor.
- Any use that could generate more than minimal additional expense to the government.
- The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data that includes privacy information, copyrighted, trademarked, material with other intellectual property rights (beyond fair use), proprietary data, or export-controlled software or data.
- Open attachments when accessing non-CBP mail systems. Opening attachments in a non-CBP mail system presents a security risk of introducing viruses, Trojans, or other malicious code into the CBP network.
- Use of official email addresses for other than official CBP business communications and signing up or registering for unapproved mailings or services.

A more complete list of inappropriate uses is contained in DHS MD 4600.1 and CBP Directive 5230-031A.

Inappropriate use is considered a security incident. Depending on its severity, the incident may be deemed a security violation and, as such, be reportable under the CBP SOC as described in DHS 4300A Attachment F, *Incident Response*.

Failure to adhere to CBP personal use policies can also result in sanctions. CBP employees and contractors may be subject to disciplinary action for failure to comply with CBP security policy, whether or not the failure results in criminal prosecution. Information security-related violations are addressed in the CBP Standards of Conduct and Tables of Offenses and Penalties. Additional violations are listed in the Standards of Ethical Conduct for Employees of the Executive Branch

Employees should NOT expect privacy when using Government resources. A banner message indicating this policy will be displayed on the login screens of CBP computers. This information will also be included in the Rules of Behavior that users are required to sign on an annual basis.

4.3 Physical Security

CBP security personnel must address physical security as an integral element in the effective

implementation of an information security program. The Office of Professional Responsibility develops and publishes the CBP Physical Security Handbook 1400-02C, which addresses physical security for CBP.

4.4 Production, Input, Output/Information Handling

Regardless of method, transmission of sensitive information should be sent through means that limit the potential for unauthorized public disclosure. The table below provides instructions for marking and handling of sensitive information.

Table 4.4: Information Handling Policies by Classification Level

Category	Definition	Handling	Marking
Classified National Security Information	Information that has been determined, pursuant to E.O. 13526, as amended, to require protection against unauthorized disclosure: and marked to indicate its classified status	Data access requires both a proper security clearance and a need-to-know. Any media containing classified material must be properly stored in a GSA-approved safe when not in use and generated on authorized computer systems	Depending on level of damage to national security, Top Secret, Secret, Confidential, standard marking applies as defined in E.O. 13526, as amended, Section 1.6, *Information Systems Security Policy Hierarchy*
For Official Use Only (FOUO)	The DHS caveat to identify unclassified information of sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs or other programs or operations essential to the national interest	Information not releasable to the public shall be controlled, handled, and processed to ensure that only authorized users with a need-to-know can access the data (keep stored in bar lock or key lock cabinets, or in areas not accessible to unauthorized personnel) additional handling procedures as defined in the DHS MD 11042.	"FOR OFFICIAL USE ONLY" Additional markings and or disclaimers may apply as needed. See Law Enforcement Sensitive Information below.

Category	Definition	Handling	Marking
Law Enforcement Sensitive (LES) (Note: LES is a subcategory under FOUO)	No DHS standard definition. Typically, investigative information, records, TECS NCIC information etc.	The same handling procedures as FOUO.	Information containing specific types of FOUO may be further marked with the applicable caveat e.g. "FOR OFFICIAL USE ONLY" This document contains Law Enforcement Sensitive Information.
Procurement Sensitive (Note: Procurement Sensitive is a subcategory under FOUO)	No DHS standard definition. Sensitive procurement information that is restricted to individuals with a need to know.	The same handling procedures as FOUO.	Materials containing specific types of FOUO may be further marked with the applicable caveat e.g. "FOR OFFICIAL USE ONLY" This document contains Procurement Sensitive Information.
Sensitive Security Information (SSI)	Information that would be detrimental to transportation security if publicly disclosed and as defined in 49 CFR 1520.5 (b)	Generally the same handling procedures as FOUO. See MD 11056 for specific handling procedures.	Information designated, as SSI shall be marked in accordance with 49 CFR 1520.13 e.g. SSI and SSI marking disclaimer.

Sensitive Security Information

Sensitive Security Information, as defined in 49 CFR 1520, is information that would be detrimental to transportation security if publicly disclosed. Sensitive Security Information is not classified information, however, there are clear procedures for recognizing, marking, protecting, sharing, and destroying Sensitive Security Information.

The Transportation Security Administration (TSA) Administrator is the delegated authority within DHS for the implementation, management, and oversight of the Sensitive Security

Information program. CBP is required to establish a viable Sensitive Security Information program. These responsibilities are defined in DHS Management Directive 11056, Sensitive Security Information.

4.5 Hardware and Software

CBP must be cognizant of the threats and vulnerabilities associated with hardware and software installation and maintenance on IT systems.

Waivers to the requirements contained in the hardening guides should be requested using DHS 4300A Attachment B *Information System Waiver and Risk Acceptance Requests.*

Policy ID	CBP Policy Statements	Relevant Controls
4.8.8.a	CBP ensures that DHS information systems follow the hardening guides for operating systems and the configuration guides for applications published by DHS CIO. *DHS 4300A Sensitive Systems Handbook* includes the DHS Secure Baseline Configuration Guides.	CM-2 CM-6
4.8.8.b	CBP limits access to system software and hardware to authorized personnel.	AC-3 CM-5
4.8.8.c	CBP tests, authorizes, and approves all new and revised software and hardware prior to implementation in accordance with their Configuration Management Plan.	CM-2 CM-3
4.8.8.d	CBP manages systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches, and eliminating or disabling unnecessary services. When the technology is available, CBP ensures that their systems are protected against pass the hash and lateral movement vulnerabilities.	CM-3 RA-5
4.8.8.e	Maintenance ports are disabled during normal system operations and enabled during approved maintenance activities.	MA-1
4.8.8.f	System libraries are managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.	SI-7
4.8.8.g	CBP develops maintenance policy and procedures.	MA-1
4.8.8.h	If cleared maintenance personnel are not available, a trusted CBP employee with sufficient technical knowledge to detect and prevent unauthorized modification to the information system or its network monitors and escorts the maintenance personnel during maintenance activities. This situation only occurs in exceptional cases. CBP takes all possible steps to ensure that trusted maintenance personnel are available.	MA-5
4.8.8.i	Maintenance using a different user's identity may be performed only when the user is present. The *user* logs in and observes the	MA-5

Policy ID	CBP Policy Statements	Relevant Controls
	maintenance actions at all times. *Users do not share their authentication information with maintenance personnel.*	
4.8.8.j	CBP defines and utilize a process for the scheduling, performance, approvals, documenting, testing, and clearing of equipment requiring maintenance. The process protects sensitive information by requiring authorized personnel to explicitly: a) Approve the removal of an information system or system components from organizational facilities for off-site maintenance or repairs b) Sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs c) Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.	MA-2
4.8.8.k	CBP approves, controls, and monitors information system maintenance tools.	MA-3
4.8.8.l	CBP obtains information system maintenance support and/or spare parts within CBP defined time period after failure.	MA-6
4.8.8.m	CBP includes requirements for software assurance and supply chain risk management prior to acquisition of any hardware or software products.	---
4.8.8.n	CBP ensures that COTS hardware and software products in use by or being considered for use in moderate and high criticality systems, are analyzed for supply chain risk prior to acquisition activities that procure new products, upgrade existing products, or that integrate these products with commercial services.	---
4.8.8.o	Employees do not use personally owned equipment or software to process, access, or store sensitive information without the prior written approval of the AO. This includes laptops, wireless mobile devices, portable data storage devices, and software.	AC-20
4.8.8.p	A property pass accompanies all equipment that enters or leaves the National Data Center, regardless of ownership of the equipment. Detailed information can be found in the CBP Physical Security Handbook (HB 1400-02C).	PE-16

4.6 Storage Media

Storage media that contain sensitive information must be controlled so that the information on the media is protected.

Storage
Proper storage of media enhances protection against unauthorized disclosure. There are additional security risks associated with the portability of removable storage media. Loss, theft, or physical damage to disks and other removable media can compromise the confidentiality, integrity, or availability of the data contained in this media.

Marking
It is recommended that a label be affixed to PCs, terminals, and laptop computers and other mobile computing devices not authorized to process classified information, especially in environments where both sensitive information and classified information are processed. Labels stating "this medium is unclassified" are available from GSA (standard form 710).

Sanitization
NIST SP 800-88 defines sanitization as the removal of data from storage media such that there is reasonable assurance the data cannot be easily retrieved and reconstructed. Sanitization methods include clearing, purging, and destruction.

Policy ID	CBP Policy Statement	Relevant Controls
4.3.a	CBP personnel, contractors, and others working on behalf of CBP are prohibited from using any non-government issued removable media (such as USB drives, in particular) and from connecting them to CBP equipment or networks or to store CBP sensitive information.	MP-2 MP-4 PE-1
4.3.b	All CBP USB drives uses encryption in compliance with DHS/CBP policy.	IA-7 SC-13
4.3.c	Users ensure proper protection of printed output. Printing of sensitive documents occurs only when a trusted person is attending the printer.	SI-12
4.1.2.d	CBP maintains records of the sanitization and disposition of information systems storage media.	MP-6

4.7 Removable Media

CBP approved removable media (e.g. thumb drives, external hard drives, SD cards, etc.) are permitted for use within the agency. Users must only use the CBP approved removable media located in the CBP TRM, unless a waiver has been granted by the CISO.

Policy ID	CBP Policy Statement	Relevant Controls
4.7.a	Approved removable media (e.g. thumb drives external hard drives, SD cards, etc.) use encryption that is FIPS 197 (AES-256) compliant and has received FIPS 140-2 validation.	MP-2
4.7.b	All CBP approved removable media (e.g. thumb drives, external	SA-9

	hard drives, SD cards, etc.) should be stored securely. In addition, all content on thumb drives is encrypted.	
4.7.c	Computer storage media, i.e., tapes, disks, removable drives, etc. containing FOUO information are marked "For Official Use Only" – per DHS MD 11042.1.	MP-2
4.7.d	Any system which removable media is connected to has the AutoRun and AutoPlay functions disabled for these devices.	CM-6
4 .7.e	All CBP thumb drives are centrally tracked and assigned to an individual, and not a group of users. For groups requiring the use of thumb drives approval of the CISO is required.	MP-2

4.8 Voice Communication Security

This section addresses vulnerabilities inherent in voice communications and the operational controls needed to mitigate the risks associated. Voice communication security encompasses Private Branch Exchange (PBX) systems, telephone usage, and voice mail. Note: If encryption is used for voice communication, AES encryption per FIPS 140-2 must be used.

Private Branch Exchange

PBXs and other voice communications switches must be tested periodically for the existence of vulnerabilities that would permit unauthorized access to sensitive information or systems, theft of service (toll fraud), loss of revenue, or legal problems. Depending on the manufacturer of the PBX and the features available, other vulnerabilities may need to be evaluated. Annual PBX evaluations will be documented in the risk assessment for the overall system.

Policy ID	CBP Policy Statement	Relevant Controls
4.5.a	CBP evaluates its PBXs annually for vulnerabilities associated with user features.	CM-2
4.5.b	CBP restricts physical and logical access to authorized personnel with a valid need-to-know.	AC-6
4.5.c	CBP communications via telephone, cell phone, facsimile, video teleconference, or voice mail do not contain information that is considered classified national security information.	PL-4
4.5.d	CBP has in place transmission protections that are commensurate with the highest level of sensitivity of the information to be transmitted. Where possible, encrypted channels or hard-wired telephones are preferred for transmission of Sensitive but Unclassified (SBU) voice communications.	CM-6
4.5.e	CBP does not store any sensitive information in voice mailboxes.	PL-4

4.9 Wireless Communications

Wireless communications technologies include wireless systems, wireless mobile devices, wireless tactical systems, and Radio Frequency Identification (RFID).

4.9.1 Wireless Mobile Devices

Wireless mobile devices include portable devices that store and transmit data, and can include voice communication capabilities such as, smartphones, tablets, and smart watches produced by any manufacturer. The term Mobile Device as defined in the National Institute of Standards (NIST) Special Publication 800-53r5, does not include laptops. The following characteristics are derived from the NIST Special Publication (SP) 8001241 and define the mobile device baseline:

- Small form factor
- At least one wireless network interface for network access (data communications). This interface uses Wi-Fi, cellular networking, or other technologies that connect the mobile device to network infrastructures with connectivity to the Internet or other data networks.
- Local built-in (non-removable) data storage
- An operating system that is not a full-fledged desktop or laptop operating system
- Applications available through multiple methods (provided with the mobile device, accessed through web browser, acquired and installed from third parties)

Policies specific to wireless mobile devices are detailed in DHS 4300A Attachment I *Sensitive Mobile Devices*.

All CBP mobile devices are enrolled in the CBP Mobile Device Management (MDM) system and controls are in place to disable their use should an outside entity attempt to reuse. However, sophisticated forensic tools have the ability of restoring data from a mobile device, even after the factory reset action has been taken. This poses a security risk to the organization so additional policy is required to safeguard CBP systems and data

Policy ID	CBP Policy Statement	Relevant Controls
4.6.1.a	Approval to use these devices are granted by the CISO. Denial/approval for use may be based on the particular CBP environment in which the device is proposed for use, as well as the nature of the data to be stored on the device.	MP-2
4.6.1.b	Government-furnished wireless mobile devices may never be connected to non-CBP devices or used for classified data.	AC-19
4.6.1.c	Government-furnished wireless mobile devices can only be used in conjunction with CBP networks or systems (to include any downloading of data from a computer workstation to these devices) if the current Security Authorization documentation specifically addresses the inherent risks associated with their use. Use of such devices are specifically authorized by the AO, who evaluates and makes the decision to accept the residual risk of use in the CBP environment.	AC-19
4.6.1.d	Government-owned wireless mobile devices may be used for SBU CBP information. Government-owned wireless mobile devices may be connected to a CBP computer system that processes sensitive information, but not classified information, to perform file sharing,	AC-19

	or for the updating of calendars.	
4.6.1.e	All wireless mobile devices have timeout mechanisms activated that automatically prompt the user to enter a password after a period of inactivity.	AC-19
4.6.1.f	Wireless mobile devices that have audio, video recording, and/or transmission capabilities are prohibited without the approval of the AO.	AC-19
4.6.1.g	Anti-virus software is used on wireless mobile devices and workstations that are used to synchronize/transmit data. The network infrastructure updates antivirus software for all applicable wireless mobile devices and their supporting desktops.	AC-19
4.6.1.h	Government-owned wireless mobile devices are treated as any other computer system or technology and are either accredited or included in the Technical Reference Model as part of the technology insertion process in accordance with DHS and CBP security policy. Any CBP computer or computer network that will have a wireless mobile device connected to it is approved through the security authorization process.	AC-19
4.6.1.i	Government wireless mobile devices conform to a CBP-approved set of configuration parameters and settings.	AC-19
4.6.1.j	The information stored on individual wireless mobile devices are evaluated during the security authorization process to determine the sensitivity of the information to be stored. If the AO considers the information to be highly sensitive, the information is encrypted utilizing commercially available FIPS 197 (AES-256) compliance and receive FIPS 140-2 validation.	AC-19
4.6.1.k	Government-owned wireless mobile devices have all files properly sanitized before being reused by another individual or office within CBP or before their disposal.	---
4.6.1.l	In alignment with CBP and DHS policies regarding enhanced retention and preservation of electronic records, CBP mobile device users must complete the following steps before returning a government furnished mobile device: 1. CBP mobile device users must appropriately file or forward any records created on their device, including all text messages, photos, video/audio recordings, and files, to an approved accessible location and comply with the preservation request, including legal holds and FOIA requests. 2. Complete an Electronic Device Record Retention Attestation (CBP form 233) and obtain a supervisor signature. 3. Submit completed CBP form 233 via “Submit” button on the form	---

4.6.1.m	Mobile devices may be reused within CBP after the device has been wiped and reset to factory settings by CBP's MDM system. This process is initiated with a "Service Catalog Task" ticket within CBP's Technology Service Desk portal (e.g. ServiceNow).	---
4.6.1.n	The device holder (individual to whom the device is assigned) shall request the "device wipe" be performed by the CBP MDM system prior to powering down and turning in the device for reuse or disposal. If the device holder is unable to initiate this action, the Local Property Officer (LPO), Wireless Account Custodian, or other designee can request in their stead. The device must remain accessible to the MDM (powered on and connected to CBP Wi-Fi or cellular service) to fully consume the wipe command.	---
4.6.1.o	Sanitization and disposal techniques must comply with NIST 800-88 Guidelines for Media Sanitization which include: disintegrate, pulverize, melt, incinerate, or shred. Magnetic media degaussers are not an acceptable method of sanitization for mobile devices.	---
4.6.1.p	Mobile devices, approved for sanitization and disposal must be done via an environmentally safe manner to protect human health and the environment.	---
4.6.1.q	Users should never attempt to shred or pulverize mobile devices, as contact with the internal battery can lead to explosion and/or fire, posing a health and safety risk to the user. Users shall request assistance from the LPO or designated personnel for disposal.	---
4.6.1.r	The office will use certified R2 or e-Steward recyclers in accordance with CBP Personal Property Asset Management policy when local disposal is authorized.	---
4.6.1.s	CBP LPOs will ensure a ticket number (e.g. ServiceNow) is referenced for each mobile device as the sanitization documentation. Additionally, all mobile devices on the affected SF120 will be destroyed, and this will be clearly identified on the CBP Form 7610, which shall be completed by the asset owning Office.	---
4.6.1.t	Mobile devices may not, under any circumstances, be donated, sold, or traded-in to any external CBP entity. This includes all manufacturer buyback programs.	---

4.10 Wireless Settings for Peripheral Equipment

Peripheral equipment (e.g., printers, scanners, fax machines, etc.) often includes capabilities, intended to allow wireless access to these devices. These wireless capabilities allow the communication over radio frequency (RF), infrared (IR), Bluetooth (BT) and 802.11x (Wi-Fi) wireless technology to create peer-to-peer, Personal Area Network (PAN) connections or other types of convenient, but insecure, methods. In general, wireless access protocols on peripheral devices shall be disabled on CBP Government Furnished Equipment (GFE) and CBP networks

unless approved by the CBP CISO and documented in the security plan of a CBP authorized FISMA system

Policy ID	CBP Policy Statement	Relevant Controls
4..a	CBP ensures that wireless capabilities for peripheral equipment are disabled. This applies all to peripherals connected to any CBP network or to systems processing or hosting CBP sensitive information.	CM-7
4.7.b	In cases where valid mission requirements or equipment limitations prevent disabling wireless capabilities, CBP complies with all requirements outlined in this policy book and DHS4300A *and* obtains a waiver in accordance with this policy.	CM-7 IR-4

4.11 Wireless Input Peripheral Devices

CBP defines wireless input devices (WID) as data input devices that connect to workstation data processing equipment without the use of a cable but do not store or process data. WIDs allow the user to communicate with computers, tablets and laptops via USB dongle transmitter/receiver connectors and uses wireless technology protocols: radio frequency (RF), infrared (IR), Bluetooth (BT) or 802.11.x (Wi-Fi). WID examples include, but are not limited to, digital signature pads, trackball/optical mice, keyboards, audio headsets, and passive video display monitors. CBP considers WIDs with no processing capabilities to be low risk devices.

Policy ID	CBP Policy Statement	Relevant Controls
4..a	In general, CBP permits the use of low risk WID peripheral equipment using RF, IR and BT technologies. WIDs may be either GFE or personally owned. 802.11x Wi-Fi and peer-to-peer capabilities are prohibited unless approved by the appropriate system ISSO and CBP CISO.	CM-7 SA-9
4.7.b	WID technology must be evaluated and approved by the CBP Cybersecurity Directorate, documented on the CBP Technical Reference Model (TRM) and listed in “Permitted” status. CBP Cybersecurity Directorate and/or ISSOs may at any time limit, restrict or otherwise withdraw the approval of specific products and technology based on unacceptable risks developed during product testing, evaluation and/or use.	CM-3 RA-5
	WID technology must be configured in accordance with DHS/CBP configuration guidance to mitigate any additional risks. ISSOs will provide configuration guidance and direction.	CM-6 CM-7
	WIDs are prohibited in areas where critical sensitive mission data is	CM-7

	discussed such as fusion centers and other highly sensitive partner areas (e.g., SCIF's) that may restrict WIDs.	

4.12 Personally Owned Equipment and Software

Users shall not use personally owned equipment (e.g., laptops, computers, wireless mobile devices, etc.) or software to process, access, or store sensitive information. Such equipment also includes plug-in and wireless (e.g., BlackBerry) peripherals that may employ removable media (e.g., CDs, DVDs). Also prohibited are USB flash (thumb) drives, external drives, diskettes, and other storage media. Waivers require written approval from the AO and will only be made when the AO deems that the use or connection is essential to the Department's mission. The AO accepts any risk associated with personally owned equipment and this residual risk must be documented as part of the system's Security Authorization Process.

CBP is required to conduct semiannual reviews of all equipment and software to ensure that only Government-licensed software and equipment are being used, or that appropriate waivers have been documented.

This policy augments the policies outlined in CBP Directive No. 1450-26 Use of Secure Messaging Platforms, June 29, 2023

- Annex A, Use of Secure Messaging Service and Multimedia Messaging Service; Limited Use of Personal Devices, August 28, 2024

Policy ID	CBP Policy Statement	Relevant Controls
4.8.a	Personally owned equipment (including mobile devices), and software are not used to process, access, or store sensitive information without the written prior approval of the AO. Any approved personally owned USB-based storage devices use encryption that is FIPS 197 (AES-256) compliant and has received FIPS 140-2 validation.	CM-10 CM-11 AC-19
4.8.b	Equipment (including wireless mobile devices) that is not owned or leased by the Federal Government or operated by a contractor on behalf of the Federal Government, shall not be connected to CBP equipment or networks without the written prior approval of the CISO. This specifically includes use of the Universal Serial Bus (USB) port to upload or download data to/from a CBP-owned device. Personally owned, low risk peripherals (e.g., passive display monitors, wireless keyboards, wireless mice and wireless audio headsets) are exempt provided these devices are listed on the CBP Technical Reference Model (TRM) in permitted status and configured in accordance with Attachment Q1—Wireless Systems."	SA-9 AC-19

4.8.c	CBP personnel do not introduce any information system asset into the CBP computing environment and/or information infrastructure, nor do they process any CBP data on any information system asset or resource device that has been obtained by DHS, CBP, any other DHS component, or any other governmental or non-governmental entity through the means of civil or criminal asset forfeiture.	AC-20
4.8.d	Use of these devices may be approved on a case-by-case basis by the AO. Any personally owned wireless mobile device used has encryption that is FIPS 197 (AES-256) compliant and receives FIPS 140-2 validation. However, approved personal wireless mobile devices used with sensitive CBP systems has all files sanitized as part of the personnel exit procedure when leaving CBP employment. Sensitive files are also sanitized when an employee changes position to another duty position that does not require the sensitive data stored on the wireless mobile device.	AC-19
4.8.e	AO approves the use of other add on devices, such as cameras and recorders. Functions that can record or transmit sensitive information via video, infrared (IR), or radio frequency (RF) are disabled in areas where sensitive information is discussed.	AC-19

Personally Owned Equipment and Software Responsibilities

AO

- Carefully evaluate the risk associated with authorizing the use of personally owned equipment or software.

CISO

- Enforce CBP policy prohibiting the use of personally owned equipment or software to connect, process, store, or access sensitive information and systems.

ISSO

- Enforce CBP policy prohibiting the use of personally owned equipment to connect, process, store, or access sensitive information and systems.
- Conduct reviews, at least semiannually, of all equipment and software in their respective offices to ensure that only Government-licensed software and equipment are being used.
- Ensure that rules of behavior address policy regarding the use of personally owned equipment and software.
- Ensure that security awareness sessions address policy regarding the use of personally owned equipment and software.

Users

- Adhere to CBP policies prohibiting the use of personally owned equipment and software.

4.13 DHS and CBP Information Security Operations

Logging and Monitoring
The DHS ESOC shall maintain visibility into security operations by using logging and monitoring. The DHS ESOC logging strategy can be broken into two main elements: real-time Security Incident Management (SIM) logging and monitoring, and archive logging designed for offline processing and later retrieval in the event of a security incident.
Effective DHS security event logging capability requires SOC and component asset integration, requisite event visibility, retention, storage considerations and direction for components to provide logging events into the DHS ESOC toolset and relevant security policy reference.
Department logging guidance is documented in the DHS Logging Strategy in the Department of Homeland Security (DHS) Security Operations Concept of Operations (CONOPS).

Authority and Management
Security operations oversight and management is inherently a governmental responsibility, not one that can be outsourced solely to contractors. While the SOC may contract for security operation capabilities, the responsibility and ultimate authority must lie with a Government employee. The Governmental authority, commonly assigned as a federal SOC manager and one or more Watch Officers, must have the ability to make decisions on behalf of the government to respond to the ever-changing cyber threat landscape. This is not an authority that can be delegated.
The federal SOC manager and at least one government Watch Officer must be cleared to Top Secret/Specially Compartmented Information (TS/SCI). Ideally all Watch Officers will be TS/SCI cleared. This is necessary to receive threat intelligence updates at TS and above.
As cyber operations are a continuous activity, governmental authority must be available continuously. This commonly is handled in the creation of three or more watch officers on an 8 hour shift rotation, or governmental authority passed from one SOC to another to cover their watch area during off-hour operations. A DHS Watch Area must never be without governmental oversight [within the chain of authority.

Forensics
Forensics is "…the examination of computer systems and the digital information created and stored on such systems to extract and analyze evidence in support of an investigation*5*."
Whenever a system compromise occurs, a computer forensic investigation will reveal whether or not the network or system has become a target of criminal action or has been used in the commission a crime Forensic investigation can protect against future incidents by revealing vectors and methods of intrusion, thus suggesting measures which can be taken to protect against future incidents.

The DHS ESOC, in cooperation with involved CBP, will conduct computer forensic examinations as deemed necessary in accordance with the incident response guidelines detailed in DHS 4300A Attachment F, *Incident Response.*

The DHS ESOC will coordinate support from CBP with appropriate capabilities for support in handling incidents requiring computer forensics.
Any investigation that reveals potential criminal activity must be turned over to the appropriate authority. Forensic investigations will normally consist of three tiers, as depicted in the table below.

Forensic Investigations Tiers

Tier	Action	Resolution
Tier 1	The CBP or DHS ESOC initiates the investigation	The CBP or DHS ESOC completes the investigation within their own capabilities, expertise, and authority.
Tier 2	CBP or DHS ESOC investigators contact the DHS ESOC Forensics Response Team for procedural, legal, or forensic capability advice as necessary.	In cases where no criminal activity is found, the SOC investigators will complete their investigation and report results to the DHS ESOC. Because the nature and complexity of investigations varies, it is impossible to establish a standard timeline for completion. Investigators must make all attempts to complete investigations as quickly as possible, without sacrificing thoroughness. Status updates shall be provided to the DHS ESOC during the weekly conference call.
Tier 3	DHS ESOC investigators discover potential criminal activity and pass the investigation to the appropriate authority after coordinating with the DHS CIO and DHS CISO.	In cases of potential criminal activity, investigators will notify the Forensics Response Team and defer investigation management to the team. The appropriate organizational team lead will assume responsibility for the investigation based on the nature suspected criminal activity. CBP and DHS ESOC investigators will provide expertise as appropriate.

4.14 Vulnerability Management

Vulnerability management is a combination of detection, assessment, and mitigation of weaknesses within a system. Vulnerabilities may be identified from a number of sources, including reviews of previous risk assessments, audit reports, vulnerability lists, security advisories, and system security testing such as automated vulnerability scanning or security control assessments.

The DHS ESOC takes a proactive approach to vulnerability management including detecting vulnerabilities through testing, reporting through ISVM messages, and conducting Vulnerability Assessments (VA).

A core element of vulnerability management is mitigating the discovered vulnerabilities, based on a risk management strategy. This strategy accounts for vulnerability severity, threats, and assets at risk.

Risk calculation will allow CBP to prioritize remediation actions, in accordance with specific situations and risk management strategies. Remediation actions will be captured in CBP's patch management policy.

Policy ID	CBP Policy Statement	Relevant Controls
4.14.a	Any CBP computer accounts (object in Active Directory (AD)) not connected to the CBP network after 45 consecutive days will be disabled. Accounts will be removed if not connected after 60 consecutive days.	---
4.14.b	All computer accounts must be created in AD for all CBP systems and must remain an object in AD to ensure adequate security controls and visibility. Operational exceptions are approved **only** by the CBP Chief Information Security Officer (CISO).	---

4.15 Information and Data Backup

Adhering to requirements regarding data backups can significantly reduce the risk that data will be compromised or lost in the event of a disaster or other interruption of service. A Backup Operations Plan must be included in the Contingency Plan.

Policy ID	CBP Policy Statement	Relevant Controls
4.15.a	The policies in this document, including Security Authorization Process requirements, apply to any device that process or host CBP data.	---
4.15.b	The CISO determines whether or not automated process devices should be included as part of an information system's Security Authorization Process requirements.	---
4.15.c	All data is backed up daily to avoid losing critical data required to support the CBP mission. CBP implements and enforces backup procedures as part of their contingency planning. CBP data backup strategies and guidance are detailed in Sections *Backup Strategy* and *Local Area Network Backup Guidance*.	CP-9
4.15.d	All portable backup media in transit use encryption in compliance with Section 5.7.1 of this Policy Directive.	CP-9
4.15.e	CBP follows the procedures established by DHS Management Directive (MD) 11042.1, Safeguarding Sensitive but Unclassified (For Official Use Only) Information, for the transportation or mailing of backup media.	MP-5
4.15.f	Backup media is shipped using an accountable delivery service (e.g. U.S. Postal Service First Class Mail, Federal Express, United Parcel Service) and shall be properly inventoried.	CP-9 MP-5
4.15.g	Every information system has a documented chain of custody process for the handling and transportation of portable backup media.	MP-5

Development of a data backup strategy begins early in the system life cycle when the c*riticality*

and sensitivity of the system are first considered. The following factors (derived from the Risk Assessment and documented in the CP) drive the data backup strategy:

- Application restoration priorities based on DHS mission criticality
- The maximum downtime permissible before DHS mission requirements are seriously degraded
- The number of data updates that can be lost between a service interruption event and the last data backup
- The number of changes in system configuration settings that can be lost between a service interruption event and the last data backup
- Interdependencies with other systems
- Identity of the System Owners

Elements that must be considered as part of the backup operations strategy include:

- Specific needs of the site
- People: their roles, responsibilities, and skill levels
- Hardware requirements
- Communications considerations
- Supplies required
- Location and availability of an alternate processing site
- Transportation requirements
- Space requirements of the recovery site
- Power and environmental requirements
- Backup documentation requirements

The frequency of backups will depend upon how often the data processed by the system(s) changes and how important the changes are. The risk assessment will drive this element of the backup strategy. Data backups must be stored both on-site and off-site, in secure facilities, in fireproof and waterproof containers.

Data backup and restoration procedures must be tested regularly as an integral part of the overall Contingency Plan. Backup copies are tested to make sure they are actually usable for restoration. More frequent testing may be required, commensurate with the risk and magnitude of loss or harm that could result from disruption of information processing support. Testing helps ensure that each person with data backup responsibilities understands and is able to technically fulfill their backup and recovery duties. Testing of data backup and restoration procedures must be formally documented, and records of testing must be retained as part of the system history.

The same principles that govern backup of system data also apply to individual users. Virtually all DHS employees and contractors will frequently possess critical sensitive data residing on hard drives on Government-owned computers or laptops. Hard drive crashes combined with failure to save critical files can result in a negative impact on the DHS mission or, at a minimum, can result in additional costs and lost time to recover or duplicate lost data. Critical data should never be kept on individual hard drives unless a backup copy exists. The backup should preferably be stored on a network drive where frequent backups are made. DHS system

administrators do not have the responsibility or the resources to assist users in recovering lost data resulting from hard drive crashes unless the System Owner deems that said data is critical to a DHS mission.

Information and data backup responsibilities are provided below:

CISO

- Establish and enforce backup policy.
- Provide technical expertise and evaluate the effectiveness of backup approaches.

Security Control Assessor

- Ensure that a Backup Operations Plan is included in the Contingency Plan.

System Owner

- Ensure that a backup strategy and procedures are established, implemented, and tested in accordance with the contingency plan.

System/Network Administrator

- Ensure that regular (daily, weekly, monthly) backups are performed in accordance with system requirements.
- Ensure that analyses are performed to determine the volume of data to be backed up, frequency of data modifications and updates, and access needs of the user community.
- Maintain a proper rotation strategy for backups.
- Ensure that all backup tapes are properly labeled in accordance with the highest data sensitivity level assigned to the system.
- Ensure that on-site and off-site backup storage locations are available.
- Ensure that on-site backups are stored in fire and water-proof containers.
- Ensure that at least one backup copy of system software is retained off-site.

ISSO

- Ensure that a Backup Operations Plan is included in the Contingency Plan.
- Ensure that the Backup Operations Plan is tested at least annually and more frequently if the risk and magnitude of loss is sufficient to warrant doing so. Ensure that timely corrective actions are taken to address deficiencies discovered during testing.
- Ensure that on-site and off-site backup storage locations are available, that on-site backups are stored in fire and water-proof containers and that at least one back-up copy of system software is retained off-site.
- Ensure that users are apprised of their responsibilities with regard to backing up any sensitive data residing on their hard drives.
- Review the Contingency Plan as part of the security authorization process.
- Ensure users and system administrators understand their responsibilities and are aware of negative impacts that can result from failing to adequately back up critical data

- Ensure the Contingency Plan, including backup procedures, is tested at least annually and that timely corrective action is taken to address deficiencies discovered during testing.
- Ensure that all testing is formally documented and ensure that records are maintained as part of the system history.

User

- Understand the critical nature of backing up sensitive data.
- Never keep critical data on individual hard drives unless a backup copy exists, preferably on the network.
- Keep supervisors apprised of projects in which critical data may not be adequately backed up.

4.16 Backup Strategy

Development of a data backup strategy begins early in the life cycle when the criticality/ sensitivity of the system is first considered. The following factors (derived from the Risk Assessment and documented in the Contingency Plan) will drive the data backup strategy:

- Application restoration priorities based on CBP mission criticality
- The maximum amount of permissible downtime before CBP mission requirements are seriously degraded
- The amount of data updates that can be lost between a service interruption event and the last data backup
- The amount of changes in system configuration settings that can be lost between a service interruption event and the last data backup
- Interdependencies with other systems
- Who the system owners are

Elements that must be considered as part of the backup operations strategy include:

- Specific needs of the site
- People, their roles, responsibilities, and skill levels
- Hardware requirements
- Communications considerations
- Supplies required
- Location and availability of an alternate processing site
- Transportation requirements
- Space requirements of the recovery site
- Power and environmental requirements
- Backup documentation requirements.

The frequency of backups will depend upon how often the data processed by the system(s) changes and how important those changes are. Again, the risk assessment will drive this element of the backup strategy.

Data backups will be stored on-site temporarily (not to exceed 30 days) in a waterproof, fireproof safe for media until the tapes are sent off-site to a secure facility where they are to be stored in an equivalent waterproof, fireproof safe. For Type II or Type III secure facilities, as defined by the CBP Physical Security Handbook, HB 1400-02C, a fireproof and waterproof media safe with a UL class 125 1-hour fire label is required. Local LAN Administrators should determine the size of safe needed by calculating the backup tape storage space required for 30 days on site and the retention period off site.

Data backup and restoration procedures must be tested annually, as a minimum, as an integral part of testing the overall Contingency Plan. This will include testing backup copies to make sure they are actually usable for restoration. More frequent testing may be required commensurate with the risk and magnitude of loss or harm that could result from disruption of information processing support. Testing helps ensure that each person with data backup responsibilities understands and is able to technically fulfill his or her backup and recovery duties. Testing of data backup and restoration procedures needs to be formally documented, and records of testing need to be retained as part of the system history.

The same principles that govern backup of system data also apply to individual users. Virtually all CBP employees and contractors will frequently possess critical sensitive data that resides on hard drives on Government-owned personal computers or laptops. Hard drive crashes combined with a failure to save critical files can result in a negative impact to the CBP mission or, at a minimum, result in additional costs and lost time to recover or duplicate lost data. Critical data should never be kept on individual hard drives unless a backup copy exists. The backup should preferably be stored on a network drive where frequent backups are made. CBP system administrators do not have the responsibility or the resources to assist users in recovering lost data resulting from hard drive crashes unless the system owner deems that said data is critical to a CBP mission.

4.17 Local Area Network Guidance

System and Local Area Network (LAN) administrators should adhere to the following practices when performing LAN backups:

1. Each CBP office will perform and maintain backups for their respective LANs. A LAN backup includes only file/print servers.
2. All CBP email will be backed up in the common store database and retained indefinitely to meet IA requirements to recover messages for case building.
3. CBP offices with LAN systems utilizing email will incrementally backup LANs on a daily basis and maintain these backup tapes for three months before recycling.
4. In addition to the required daily backups, CBP offices will perform weekly full backups regardless of which LAN system(s) they utilize.
5. Multiple incremental backups on the same tape are allowed. It is preferred, however, that incremental daily backups be stored off-site, which would prevent multiple incremental backups on the same tape.

6. On a monthly basis, all weekly full and monthly full LAN backup tapes will be moved to an offsite tape storage facility. The weekly tapes will be maintained offsite for 1 month and the monthly tapes will be retained for 1 year. A reciprocal storage arrangement rather than use of a commercial storage site is an acceptable solution (i.e., a Field Office might use the Port Office for their off-site tape storage and the Port Office could use the Field Office). Such a reciprocal arrangement would require an appropriate number of fireproof/waterproof safes for storage of these tapes.
7. When required onsite, LAN administrators (part time, full time, Field Office, or collateral duty), will perform LAN backups, backup tape storage, and file restoration for their respective CBP office.

4.18 Converging Technologies

Advances in technology have resulted in the availability of devices that offer multiple functions. Many devices such as multifunctional desktop computers, copiers, facsimile machines, and Heating, Ventilation and Air Conditioning (HVAC) systems may contain sensitive information and may also be connected to data communications networks.

These devices shall be configured to ensure that incoming lines cannot be used to access the data network or any information retained in the memory. CBP shall use only multifunctional devices that have been evaluated and validated through accredited commercial laboratories or by NIST (e.g., the National Security Agency (NSA)/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program).

Policy ID	CBP Policy Statement	Relevant Controls
4.18.a	The policies in this document apply to any networked devices that contain information technology, including copiers, facsimile machines, and alarm control systems.	---
4.18.b	CBP ensures that network printers and facsimile machines are updated to the latest version of their firmware/software at least annually.	CM-2
4.18.c	CBP ensures that network printers, copiers, and facsimile machines shall be configured for least required functionality.	CM-7
4.18.d	CBP ensures that each network printer, copier, and facsimile machine is within the system definition of a DHS information system that has a current ATO.	CM-8 PL-2
4.18.e	CBP ensures that remote maintenance of network printers, copiers, and facsimile machines is conducted only from within DHS networks. If maintenance planning does not include performing remote maintenance, CBP ensures that remote maintenance capabilities are disabled.	MA-4
4.18.f	CBP ensures that network printers, copiers, and facsimile machines are configured to restrict administrator access to authorized	MA-5

	individuals or groups.	
4.18.g	CBP ensures that maintenance/disposal is performed on network printer, copier, or facsimile machine approved for sensitive reproduction is performed only while a properly cleared person with knowledge to detect any inappropriate escorts the maintenance technician.	MA-5
4.18.h	CBP ensures that memory and hard drives do not leave the facility; they are to be replaced and the old part destroyed as sensitive media.	MP-6
4.18.i	CBP locates network printers, copiers, and facsimile machines approved to process sensitive information in areas where access can be controlled when paper output is being created.	PE-18
4.18.j	Any multifunction device connected to a CBP network or other information system containing sensitive information has the inbound dial in capabilities disabled.	AC-17
4.18.k	CISO determines whether or not automated process devices need to be included as part of an IT system's Security Authorization requirement.	CA-2

The use of nontraditional information systems elements without appropriate safeguards presents risks to CBP organizations in part because these devices are typically not thought of as information systems.
Wireless devices must be secured as specified in this Policy Handbook and in DHS 4300A. Copiers with the capability to process sensitive documents must be secured in the same manner as facsimile machines. Sanitization of media included in high-end copiers (or other devices) must be carried out in the manner prescribed in this Policy Handbook and DHS 4300A. If the device is a multifunction device, the facsimile functions must be secured in the same manner as stand-alone facsimile machines. Printing functions must be secured in accordance with the provisions in this Policy Handbook and in DHS 4300A. HVAC, fire suppression, and power equipment (including emergency power backup) are to be secured in accordance with the requirements specified for PBX. If these do not have internal auditing functions, manual audit/access logs are to be maintained by a trusted employee who accompanies any individual who performs maintenance, upgrade or repair on the indicated systems.

The devices discussed in this section that have the capability to process or store sensitive data, whether or not such devices are connected to CBP networks, shall be clearly documented in the Security Plan and authorized for that functionality. The risks of using such devices shall be identified along with countermeasures employed to mitigate these risks. This information shall also be included in applicable rules of behavior and addressed in awareness training orientation and refresher sessions.

Responsibilities related to converging technologies are provided below:

ISSO

- Ensure that nontraditional IT components connected to sensitive systems meet the security requirements detailed in this handbook and are authorized for that purpose.
- Ensure media storage devices included in copiers, facsimile machines, printers, etc., are properly sanitized before leaving CBP control.
- Ensure audit logs are maintained and reviewed for nontraditional IT components that store or process sensitive information.

Network/System Administrator

- Protect and monitor network connections to nontraditional IT devices such as facsimile machines and copiers.

Facility Managers

- Notify and coordinate with the ISSO when facility systems (e.g., HVAC and alarm systems) require connectivity to sensitive systems.
- Ensure proper physical security is afforded to infrastructure equipment that processes, stores, or connects to a sensitive system.

5.0 Technical Policies

The design of information systems that process, store, or transmit sensitive information shall include the automated security features discussed in this section. Security safeguards shall be in place to ensure that each person who has access to sensitive information systems is individually accountable for their actions while utilizing the system.
Technical controls focus on security controls that a computer system executes. These controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. For example, user access is controlled and limited based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.

5.1 Identification and Authentication

Identification is the process of telling a system the identity of a subject. Usually this is done by entering a name or presenting a token to the system via a smart card. The identity of each user must be established prior to authorizing access to the system, and each system user must have his or her own unique User Identification (ID). Personal Identification Verification (PIV) credentials, or alternative solutions that provide NIST SP 800-63 Level of Assurance (LOA) 4 of the user's identity is the primary means of logical authentication for DHS sensitive systems. NIST SP 800-63 states that a username, password, and single factor one-time password (such as RSA SecurID) is not LOA 4 compliant.

Authentication is the process of proving that a subject is who the subject claims to be. Authentication is a measure used to verify the eligibility of a subject and the ability of that subject to access certain information. There are three methods of authenticating:

- Something you know (e.g., password)
- Something you have (e.g., a smart card)
- Something you are (e.g., a biometric such as a fingerprint)

U.S. Customs and Border Protection (CBP) systems must be designed to ensure that each user is authenticated before access is permitted. Concurrent logins to the same system or application using the same authentication credentials are not allowed, unless a specific business or operational need is documented and approved by the Authorizing Official (AO).

Policy ID	CBP Policy Statements	Relevant Controls
5.1.a	Ensure that user access is controlled and limited based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.	IA-1 IA-2
5.1.b	For information systems requiring authentication controls, CBP ensures that the information system is configured to require that each user is authenticated before information system access occurs.	IA-1 IA-2
5.1.c	For systems with low impact for the confidentiality security objective, CBP disables user identifiers after 90 days of inactivity; for systems with moderate and high impacts for the confidentiality security objective, CBP disables user identifiers after 45 days of inactivity. This policy applies to anyone who is granted account access to any network, system, or application in use in the Department.	IA-4
5.1.d	Users do not share identification or authentication materials of any kind, nor any user allow any other person to operate any CBP system by employing the user's identity.	IA-5
5.1.e	All user authentication materials are treated as sensitive material and rated as high as the level of the most sensitive information to which that user is granted access using that authenticator.	IA-7
5.1.f	Personal Identification Verification (PIV) credentials or alternative solutions that provide NIST SP 800-63-2 Level of Assurance (LOA) 4 of the user's identity used as the primary means of logical authentication for DHS sensitive systems. Per NIST SP 800-63-2, "Electronic Authentication Guideline," a username, password and single factor one-time password (e.g. RSA SecurlD) is not LOA 4-compliant.	---

Policy ID	CBP Policy Statements	Relevant Controls
5.1.g	Mandatory smart card logon is implemented by means of Identity (user) Based Enforcement. Until the end of FY15, while systems that support only username and password are updated to support PIV smartcard authentication (e.g., Integrated Windows Authentication, SAML-based Single Sign-On, Direct PK-enablement), organizations may choose to implement Machine Based Enforcement as an interim means of PIV enforcement.	IA-2
5.1.h	Privileged network users use the DHS HSPD-12 credentrial for authentication to all CBP Privileged network user accounts.	IA-2
5.1.i	Only approved DHS Privileged Network User Management solutions are employed. A waiver request is required for use of any other solution(s).	---
5.1.j	Systems prompt privileged users to enter the PIV PIN to initiate an encrypted authenticate session.	---
5.1.k	Password authentication is disabled for all accounts. Where applicable, all password-based authentication nodules are disabled. This policy applies to all IP-addressable devices.	---
5.1.l	All system access is by use of the user's PIV card.	IA-2
5.1.m	Users report lost, stolen, or inadvertently destroyed DHS PIV Cards to the DHS PCI by email at OneCardSSD@hq.dhs.gov and to the CBP Technology Service Desk (TSD), who supplies a temporary logon.	---
5.1.n	Users report forgotten or misplaced PIV cards to the TSD, who supply a temporary logon that expires 24 hours after creation. Users also report to the DHS PCI by email at OneCardSSD@hq.dhs.gov.	---
5.1.o	User credentials (user-ID plus password) are unique for each system to which a user is granted access. If the Hash ID is required as the user-ID for each system, then the password for each system must be unique.	IA-2
5.1.p	Guest/guest accounts are prohibited from being installed.	AC-2
5.1.q	No accounts are named anonymous, ftp, telnet, www, host, user, bin, nobody, etc.	AC-2
5.1.r	All User IDs are revalidated at least annually by the IT system owner or manager.	AC-2

Identification and authentication responsibilities are provided below:

Identification and Authentication Responsibilities
Chief Information Security Officer (CISO) • Establishes and enforces identification and authentication policy.

Identification and Authentication Responsibilities
• Provides technical expertise and evaluates the effectiveness of identification and authentication approaches. • Assesses technology opportunities that have the potential to enhance compliance with identification and authentication requirements. **Security Control Assessors** • Ensure that systems limit user access based on the identification and authentication of each user prior to assessing the system. **System Owners/IT Project Managers** • Ensure adequate resources are budgeted for information assurance; assess identification and authentication technology opportunities for potential application to CBP systems. **System/Network Administrators/Field Technology Officers (FTOs)** • Ensure that the system identifies every user as unique. • Enforce strong passwords or other more effective means (e.g., Public Key Infrastructure (PKI)-based keys or smartcards). • Secure and administer privileged accounts using authentication technology stronger than passwords. **Information System Security Officers (ISSOs)** • Brief users on identification and authentication procedures and protection requirements. • Monitor/enforce compliance with identification and authentication requirements. • Review and approve the initial password distribution plan which must be contained in the Security Plan (SP). • Shall obtain a list of users containing Username and Full name as part of the system self-assessment to determine compliance with the approved initial password distribution mechanism. • Perform system audits to verify compliance. **Users** • Comply with identification and authentication guidance, specifically guidance pertaining to password management. • Report violators of identification and authentication security policies as a security incident

Identification and Authentication Responsibilities
to the SOC and notify your supervisor/manager if it is a significant incident. (See DHS 4300A Attachment F, *Incident Response* for information on procedures and definitions of incidents.)

Privileged accounts are to be secured by authentication technology stronger than that based only on a User ID and password. All actions taken by privileged users with respect to systems and applications should be encrypted to prevent "playback" attacks; they must also be logged for auditing purposes. All passwords, algorithms, keys, certificates, codes, or other schemes that are used by the system for authentication purposes must be stored in a manner that prevents unauthorized individuals from gaining access to them. A system can be compromised without proper, secure storage.

5.2 Access Control

Network and system administrators ensure that access controls operate as intended. The authority delegated to these roles to add, change, or remove component devices, dial-up connections, network addresses and protocols, or to remove or alter programs should be tightly controlled. This authority should be divided among more than one administrator, supervisor or root password holder.

Users are responsible for protecting all CBP information to which they are granted access. Access controls restrict access to system objects such as files, directories, and devices based upon the identity of the user, or the group to which the user belongs. Subverting access controls violates this policy. Access controls protect against the unauthorized disclosure, modification, or destruction of the data residing in these systems, as well as the applications themselves. They offer alternative means to restrict activities of the general user population.

Automated systems are vulnerable to fraudulent or malicious activity by individuals who have the authority or capability to access information not required to perform their job-related duties. Access control policy is designed to reduce the risk of an individual acting alone from engaging in such fraudulent or malicious behavior. The Principle of Least Privilege states that users should only be able to access the system resources needed to fulfill the user's job responsibilities.

Principle of Least Privilege: Requires that each user in a system be granted the most restrictive set of privileges (or lowest clearance) needed for performance of authorized tasks.
The application of this principle *limits the damage that can result from an accident, error, or unauthorized use.*

Policy ID	CBP Policy Statements	Relevant Controls
5.2.a	CBP implements access control policy and procedures that provide protection from unauthorized alteration, loss, unavailability, or disclosure of information.	AC-1
5.2.b	Access control follows the principles of least privilege and separation of duties	AC-5

Policy ID	CBP Policy Statements	Relevant Controls
	and shall require users to use unique identifiers. *Social Security Numbers are not used as login IDs.*	AC-6
5.2.c	Users do not provide their passwords to anyone, including system/network administrators and/or Field Technology Officers.	IA-5
5.2.d	Emergency and temporary access authorization is strictly controlled and approved by the CBP CISO or his/her designee prior to being granted.	AC-2
5.2.e	System Owners ensure that users are assigned unique account identifiers.	IA-4
5.2.f	The Lock Workstation button should be used to lock the computer when leaving the workstation unattended, except for overnight.	AC-11
5.2.g	Screen savers integral to the operating system may be used to restrict access to workstations and servers. Users engage the password protection feature of their screen savers when leaving workstations or servers unattended.	AC-11
5.2.h	Servers using screen savers are advised not to use open 3GL-type screen savers that use an undue amount of processing resources.	AC-11
5.2.i	CBP systems with a Federal Information Processing Standard (FIPS) 199 confidentiality categorization of high limits the number of concurrent sessions for any user to one unless strong authentication is used.	AC-10
5.2.j	CBP ensures that all data-at-rest, particularly in cloud or other virtual environments, preserves its identification and access requirements (anyone with access to data storage containing more than one type of information have specific access authorization and for every type of data in the data storage).	---

System/network/LAN administrators/FTOs and ISSOs are responsible for ensuring that access controls are in place and operating as intended. It is especially critical that the authority to add, change, or remove component devices, dial-up connections, and network addresses and protocols, or to remove or alter programs be tightly controlled with access limited to only a select group of authorized personnel.

- **Initial User Access**

  Users who require access to CBP systems and networks must have completed a Background Investigation (BI) prior to being granted access. However, users with a Limited BI may be given access to email, the Internet, and Development and Systems Acceptance Testing (SAT) environments.

  The user's supervisor or government project manager must determine the system user's need to access a system and the levels of access required. User access will vary depending upon the position held. This authorization becomes critical to maintaining correct security measures. The system owner or designated representative must approve user access privileges.

- **Review of Access Privileges**
  User data access requirements will change over time. Therefore, supervisors or ISSOs should review access control lists to verify that they reflect who has access to what data and

ensure that access control list are up to date. This requirement also applies to contractors and other non-DHS personnel with access to any DHS systems. ISSOs have an oversight responsibility to ensure this is being accomplished. These actions are reviewed as part of the Security Authorization process and during annual self-assessments.

Access control policies and procedures need to be written down and stored in an off-site location. They need to be accessible in the event of an emergency. This information also needs to be included in the Contingency Plan.

- **Terminated and Departing Employees**
  System/Network/LAN Administrators and ISSOs must ensure that all departing employees have their access privileges terminated immediately. No former employee should have any ability to access system resources after their term of employment has ended. Procedures vary depending on whether the separation is voluntary or involuntary. Termination of access privileges also applies to employees whose job functions have changed such that they no longer require access to the level of sensitive information to which they were previously granted.
- **Secure Remote Access**
  Hardware security tokens, such as cryptographic smartcards, can be issued to CBP employees and contractors who have a valid need to remotely access CBP systems and data. Users are responsible for protecting all DHS information to which they have access. Access control responsibilities are provided below:

Access Control Responsibilities
CISO • Establish and enforce access control policy. • Provide technical expertise and evaluate the effectiveness of access control approaches. • Assess that adequate access controls are in place. • Directly approve, or delegate authority to a strictly controlled group, emergency and temporary access prior to being granted. **Security Control Assessors** • Conduct assessments to verify that adequate access controls are in place. **System/Network/LAN Administrators/FTOs** • Ensure that access controls are in place and functioning as intended. • Ensure that access controls provide the security features outlined in this document. • Ensure that systems prevent users from having multiple concurrent active sessions for one

Access Control Responsibilities
identification unless the AO has granted authority based upon operational business needs. **ISSOs** • Ensure that access controls are in place and functioning as intended. • Ensure that access controls provide the security features outlined in this document.

5.2.1 Automatic Account Lockout

CBP shall configure each information system to lock a user's account for a specified period following a specified number of consecutive failed logon attempts. Users shall be locked from their account for a minimum period of 20 minutes after three consecutive failed logon attempts during a 24-hour time period. CBP shall configure systems to require the system administrator to unlock a user's account after three consecutive failed logon attempts for systems rated as High or designated as financial systems. All failed logon attempts must be recorded in an audit log and periodically reviewed.

Policy ID	CBP Policy Statements	Relevant Controls
5.2.1.a	CBP implements and enforce an account lockout policy that limits the number of consecutive failed logon attempts to three during a 24-hour time period. Systems should lock out a user account after three consecutive failed logon attempts. All failed logon attempts are recorded in an audit log and periodically reviewed.	AC-7
5.2.1.b	CBP configures accounts to automatically lock a user's *account* after 3 consecutive failed logon attempts.	AC-7
5.2.1.c	The automatic lockout period for accounts locked due to failed login attempts are set for twenty (20) minutes.	AC-7
5.2.1.d	CBP configure systems to require the system administrator to unlock a user's account after three consecutive failed logon attempts for systems rated as High or designated as financial systems.	AC-7
5.2.1.e	CBP establishes a process for manually unlocking accounts prior to the expiration of the 20-minute period, after sufficient user identification is established. This may be accomplished through the help desk.	AC-7

Automatic account lockout responsibilities are provided below:

Automatic Account Lockout Responsibilities
CISO • Establishes and enforces automatic account lockout policies. **System/Network/LAN Administrators/FTOs** • Ensure that systems are configured to lock a user's account for 20 minutes after three unsuccessful logon attempts during a 24-hour time period.

Automatic Account Lockout Responsibilities
• Unlock a user's account after three consecutive failed logon attempts once the user is properly identified and authenticated for systems rated as High or designated as financial systems. **ISSOs** • Ensure that systems are configured to lock a user's account for 20 minutes after three unsuccessful logon attempts.

5.2.2 Automatic Session Termination

The term *session* refers to a connection between a terminal device (workstation, laptop, mobile devices, etc.) and a networked application or system. The term does not apply to a direct connection to a CBP network, such as authenticating from a device that is directly connected to a CBP network. The term *session* also refers to accessing an application or system through the CBP network, such as a database or networked application. When a session is locked, the user may resume activity by re-authenticating.

Each CBP IT system shall be configured to deactivate any user session immediately and automatically following 20 minutes of inactivity, in such a way that will require the user to re-authenticate his identity before resuming interaction with the system. The session is not terminated, but the user will need to log on again in order to activate the session. Sessions shall automatically be terminated after 60 minutes of inactivity.

For IT systems that require more than the 20-minute minimum to run queries or complete other functions, the system owner and ISSO may submit an exception to policy request justifying the extended period necessary and including other security controls in place to safeguard access control.

System owners and/or ISSO may establish a more stringent automatic session lockout policy than the minimum CBP 20-minute limit.

Policy ID	CBP Policy Statements	Relevant Controls
5.2.2.a	Network applications or systems are configured to automatically deactivate or lock any user session in accordance with the appropriate configuration guide. In the absence of configuration guidance, the session locks following 20 minutes of inactivity.	AC-11
5.2.2.b	Locked sessions remain locked until the user re-authenticates.	AC-11
5.2.2.c	Sessions automatically be terminated after 60 minutes of inactivity.	SC-10

Automatic session lockout responsibilities are provided below:

Automatic Session Lockout Responsibilities
CISO • Establishes and enforces automatic session lockout policies. • Approve any request for policy exception to extend automatic session lockout to any period beyond 20 minutes for specific IT systems with mission justification. **System/Network/LAN Administrators/FTOs** • Ensure that systems are configured to deactivate or lock any user session that has remained idle for 20 minutes. • Ensure that systems are configured to terminate any user session that has remained idle for 60 minutes. **ISSOs** • Ensure that systems are configured to deactivate or lock any user session that has remained idle for 20 minutes. • Ensure that systems are configured to terminate any user session that has remained idle for 60 minutes. • Submit request for policy exception to extend automatic session lockout to any period beyond 20 minutes for specific IT systems with mission justification.

5.2.3 Warning Banner

The DHS CISO mandates that a warning banner statement be displayed on all DHS IT systems during logon. The most current language can be found on the DHS CISO's web page located at https://usdhs.sharepoint.com/sites/dhsconnect/org/comp/mgmt/ocio/ciso/Pages/sspolicy.aspx

Please note that the current warning banner was developed specifically for use on DHS workstations. Due to differing functions, purposes and situations, and to length requirements, warning banners for other environments, such as routers, switches and public-facing websites, will be developed and included in a future version of the *DHS 4300A Sensitive Systems Handbook*.

The use of the warning banner serves as a reminder to all users that the computers they are accessing are Government computers and must be used in accordance with good security practices.

Policy ID	CBP Policy Statements	Relevant Controls
5.2.3.a	Systems internal to the DHS network displays a warning banner specified by the DHS CISO.	AC-8
5.2.3.b	Systems accessible to the public provides both a security and a privacy statement at every entry point.	AC-8
5.2.3.c	CBP IT externally facing websites accessible by the public displays a warning banner during logon and before granting users system access.	AC-8
5.2.3.d	The current language for Secret and Top Secret Computer Log-On Banners can be found on the DHS-CISO's web page located at https://usdhs.sharepoint.com/sites/dhsconnect/org/comp/mgmt/ocio/ciso/Pages/sspolicy.aspx	AC-8
5.2.3.e	CBP approves the IT system use notification message before its use in production.	AC-8
5.2.3.f	The system use notification message remains on the screen until the user takes explicit actions to log on to the information system.	AC-8

Warning banner responsibilities are provided below:

Warning Banner Responsibilities
DHS CISO • Establishes and enforces the use of appropriate standard Warning Banner and Privacy Statement for display at all internal publicly accessible entry points to DHS and CBP IT systems. **CISO** • Establishes policy compliant with DHS policy for use of appropriate standard Department

Warning Banner Responsibilities
Warning Banner applicable to all CBP IT systems. **System/Network/LAN Administrators/FTOs** • Ensure that internal IT systems under their controls are configured to display the approved Department Warning Banner. • Ensure publicly accessible IT systems under their control are configured to display the approved Department Warning Banner and Privacy Statement. **ISSOs** • Ensure that internal IT systems under their controls are configured to display the approved Department Warning Banner. • Ensure publicly accessible IT systems under their control are configured to display the approved Department Warning Banner and Privacy Statement.

5.2.4 External User Account Recertifications

CBP has a number of systems that are utilized by external users to include TECS, SEACATS, and many others. OIT identified an external user account recertification process that allows external users to be notified of their user role account prior to user access expiration. Notification requires the external user to take action and confirm if access is still needed on the selected system(s). Recertification is needed for External users with Read only access and/or privileged access (write, change, modify, delete data).

With CISO approval, software developers can be granted permanent read-only access to production applications. ISSMs, ISSOs and System Owners associated with the system are responsible for all reviews, audits, compensating controls and any artifacts related to this access. The permanent read-only access will be reviewed and reassessed in October at the beginning of every fiscal year.

Policy ID	CBP Policy Statements	Relevant Controls
5.2.4.a	External users with read only access must recertify and sign the DHS/CBP Rules of Behavior **once a year**. External users with privileged access must recertify and sign the DHS/CBP Rules of Behavior **every 6 months**.	---
5.2.4.b	In order to retain and/or regain access to the system, verification of access is required by the external user's supervisor. In lieu of a supervisor, each component must provide a liaison list for each system identifying the AO.	---
5.2.4.c	ISSMs are responsible for recertifying the list of each component annually. However, ISSMs may delegate this responsibility to the ISSO of the system.	---

Supervisory positions are also considered an employee when coded in the pay files as a 2, 4 or 5. Further explanation is listed below:

Code	Name	Explanation
2	Supervisor or Manager	Position requires the exercise of supervisory or managerial responsibilities that meet, at least, the minimum requirements for application of the General Schedule Supervisory Guide or similar standards of minimum supervisory responsibility specified by position classification standards or other directives of the applicable pay schedule or system.
4	Supervisor (CSRA)	Position meets the definition of Supervisor in 5 U.S.C. 7103(a)(10) but does not meet the minimum requirements for application of the General Schedule Supervisory Guide.
5	Management Official (CSRA)	Position meets the definition of Management Official in 5 U.S.C. 7103(a)(11) but does not meet the General Schedule Supervisory Guide definition of Supervisor/Manager or the definition of Supervisor in 5 U.S.C. 7103(a)(10).

5.3 Auditing

A fundamental computer security principle is that each person is to be individually accountable for his or her actions while using the system. By providing the ability to track a user's activities while accessing an automated system, auditing tools are an effective method of enforcing this principle. Audit trails maintain a record of system activity by both system and application processes as well as by individual user activity.

CBP personnel shall use system audit features to review CBP system and network events and security activities recorded in log files for unauthorized or inappropriate activities. The type of security events contained or captured within the audit log must be reviewed annually with additional security events being considered as necessary.

Audit trails maintain a record of system activity by both system and application processes as well as by individual user activity. In conjunction with appropriate tools and procedures, auditing can further several security-related objectives including:

- Individual accountability
- Reconstruction of events

- Intrusion detection
- Problem identification

Audit trails can track the identity of each subject attempting to access the system, the time and date of access, and the time of log off. In addition, audit trails can capture all activities performed during a session and can specifically identify those activities that have the potential to modify, bypass, or negate the system's security safeguards. The auditing technique used must be able to support after-the-fact investigations of how, when, and why normal operations ceased. Audit trail records must be maintained online for at least 90 days, thereby allowing rapid access to recent information. Audit trails should be preserved for a period of three years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease. Preservation of the audit information should be part of the IT Contingency and business continuity plans, so that events preceding a disaster or interruption of service can be reconstructed.
To be effective, audit trails must be periodically reviewed and analyzed. The need to review the information captured by the auditing process is of paramount importance. In many cases, it is only through the review process that incidents of unauthorized access, modification, or destruction are uncovered. Audit trails also need to be secured to prevent tampering and backed up regularly.

Policy ID	CBP Policy Statements	Relevant Controls
5.3.a	Audit records are sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. Audit records are reviewed as specified in the information Security Plan (SP). The audit record contains at least the following information: • Identity of each user and device accessing or attempting to access an information system • Time and date of the access and the logoff • Activities that might modify, bypass, or negate information security safeguards • Security-relevant actions associated with processing • All activities performed using an administrator's identity	AU-3 AU-12
5.3.b	Audit records for financial systems or for systems hosting or processing Personally Identifiable Information (PII) are reviewed by the system administrator monthly. Unusual activity or unexplained access attempts are reported to the system owner, CISO, and the Security Operations Center (SOC).	AU-6

Policy ID	CBP Policy Statements	Relevant Controls
5.3.c	CBP ensures that their audit records and audit logs are protected from unauthorized access, modification, or destruction.	AU-9
5.3.d	CBP ensures that audit logs are recorded and retained in accordance with CBP or DHS's Record Schedule. At a minimum, audit trail records are maintained online for at least 90 days or for a time period necessary for the review of events when system compromise occurs, whichever is longer. Audit trail records are preserved for a period of three years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease. CBP allocates appropriate audit record storage capacity in accordance with these requirements.	AU-4 AU-11
5.3.e	The system risks associated with extracts of PII from databases are evaluated. If the risk is determined to be sufficiently high, a procedure is developed for logging computer-readable data extracts. If logging these extracts is not possible, this determination is documented, and compensating controls identified in the SP.	AU-1 AU-2 AU-3 PM-9
5.3.f	The CBP Security Operations Center (SOC) implements both general and threat-specific logging.	AU-1 AU-2
5.3.g	CBP ensures that information systems alert the CBP SOC in the event of an audit processing failure and overwrite the oldest audit records, if an analysis of the mission needs and the risk to the system preclude system shutdown.	AU-5
5.3.h	CBP ensures that information systems provide an audit reduction and report generation capability that: a) Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents b) Does not alter the original content or time ordering of audit records. This capability could be as simple as a text editor that allows the administrator to produce a sorted text file, or extract data from an audit log.	AU-7
5.3.i	CBP ensures that audit logs employ a consistent time stamp across all systems.	AU-8
5.3.j	SPs for individual applications specifically address audit requirements and retention periods for system log files. Audit requirements for individual systems may specify more detailed information than the minimum listed above.	PL-2
5.3.k	Computer-Readable Extracts (CREs) involving PII are erased within 90 days unless the information included in the extracts is required beyond the 90 days.	PL-5

Policy ID	CBP Policy Statements	Relevant Controls
	Permanent erasure of the extracts or the need for continued use of the data are documented by the System Owner and audited periodically by the CBP Privacy Officer. See Attachment S1, *Managing CREs Containing SPII*.	
5.3.l	CBP systems provide mechanisms to associate an individual with a single, unique identity, which also associates a user with security-relevant events.	AU-3
5.3.m	System administrators should be assigned one account for root system tasks and a second account for routine access.	AC-6
5.3.n	Audit trail requirements cannot be waived except in extreme circumstances, and then only by the Assistant Commissioner of the Office of Information and Technology (OIT). Where this requirement is waived, other security controls such as user authentication, file passwords, magnetic media control procedures, and a logging mechanism to record terminal usage is verified and implemented.	AU-2

Auditing responsibilities are provided below:

Auditing Responsibilities
Assistant Commissioner, OIT • Authority to waive Audit Trail requirements, only in extreme circumstances. **CISO** • Ensure that all CBP IT systems maintain an audit record sufficient to reconstruct security relevant events. • Evaluate auditing requirements; budget for and select appropriate auditing tools. • Establish policy for retention of audit logs. • Ensure auditing is performed independently of system/network administration. **System Owners** • Ensure adequate resources are budgeted for implementing and maintaining an effective auditing capability. • Work with IT managers to identify critical functions to be subjected to auditing and keep apprised of auditing findings. • Ensure auditing is performed independently of system/network administration. **System/Network/LAN Administrators/FTOs** • Maintain an audit record sufficient to reconstruct security relevant events.

Auditing Responsibilities

• Ensure that the audit record includes:
  o The identity of each person and device accessing or attempting to access the system.
  o The time and date of the access and when the user logged off.
  o Activities performed using an administrator's identification.
  o Activities that could modify, bypass, or negate the system's security.
  o Sufficient detail to facilitate reconstruction if compromise or malfunction occurs.
  o Security-relevant actions associated with processing.
• Protect audit records against unauthorized access, modification, or destruction.
• Retain audit records for a minimum of 90 days or in accordance with the SP and ensure that audit records are regularly backed up.
ISSOs
• Ensure that the SP addresses accountability and auditing.
• Ensure that the risk analysis documents the rationale and justification for any CBP IT system that does not implement an auditing capability.
• Ensure that audit records include all required elements.
• Review audit records at least once per week or in accordance with the SP.
• Ensure that audit collection and review procedures contain adequate separation of duties provisions.
• Report security-relevant events to the SOC.

5.4 Network and Communications Security

Network security encompasses remote access, network monitoring, external connections, boundary protection, Internet usage, email security, and vulnerability scanning. This section addresses vulnerabilities inherent in network security and the technical controls needed to mitigate the risks associated with these vulnerabilities. This section focuses on CBP policies governing security of network access, devices, and usage.

5.4.1 Remote Access and Dial-In

Remote access technology allows trusted employees to access CBP networks by dialing in via modem or accessing via the Internet. This allows mobile employees to stay in touch with the home office while traveling away from their normal work locations. However, there are significant security risks associated with remote access and dial-in capabilities. Proper procedures can help mitigate these risks.

Unauthorized access is the biggest risk associated with remote access. Access by untrusted or uncleared persons can violate the Department's confidentiality, integrity, and availability standards. An unsecured modem or other dial-in facility could provide a backdoor to the entire DHS network for unauthorized users (inside or outside of the DHS). Malicious individuals can also exploit improperly configured remote control software.

There are commercially available products that can be used in conjunction with other network protection mechanisms to reduce the risks of unauthorized access. These require the use of authentication methods stronger than passwords and user IDs.

CBP must develop and implement acquisition procedures to ensure that only approved hardware and software is purchased and operated.

Note: Remote access solutions that do not comply with the requirements of Federal Information Processing Standards (FIPS) 140-2 are not authorized.

Virtual Private Networks

Secure Virtual Private Network (VPN) communications access capabilities must provide strong identification and authentication, audit logging, and integrity controls; and they must be implemented using a CBP-approved session level encryption mechanism designed to protect the identification and authentication process as well as data transmission.

VPNs are alternative methods for access to CBP networks and are permitted under specific circumstances, which primarily consist of an assurance that the FIPS 140-2 standard is followed, and encryption will exist to protect data transmission across unsecured networks into the CBP network. CBP-owned desktops and laptops using VPNs require CBP-approved personal firewalls to be installed. (See Section 5.7.1, *Encryption* and Section 5.4.4, *Firewalls and Policy Enforcement Points*) VPNs are primarily designed to assure secure transmission between a client desktop or laptop and a server inside CBP. Where possible, the elements of this arrangement must be owned and operated by CBP, not by a vendor company unless specifically contracted for that purpose and with prior approval of the CISO. Under such circumstances where VPNs are used to connect to external networks, an Interconnection Security Agreement (ISA) is required (See 5.4.3, *Network Connectivity and Attachment N, Preparation of Interconnection Security Agreements). All VPNs require a technical review by an ISSO, Certification Agent (CA), and approval by the CISO.*

Telework Security Policy

The U.S. Customs and Border Protection (CBP) telework security policy follows the National Institute of Standards and Technology, Special Publication 800-46 Revision 1, Guide to Enterprise Telework and Remote Access Security, to define telework and remote access requirements.

Other Remote Access Methods

Other methods to secure communication within and to CBP networks are authorized. The use of Public Key Infrastructure (PKI)-enabled smartcards, proprietary tokens, or similar methods is

authorized for use. These remote access methods must also comply with both CBP and DHS policies regarding standards-based encryption methodologies and management. If the chosen solution is PKI-based, the appropriate federal standards (e.g., FIPS or National Institute of Standards and Technology (NIST) must be used in its certification.

Alternative forms of remote access methods are not authorized. Remote access methods that include either hardware or software solutions not approved by CBP, and which have not been documented and certified by the appropriate federal authority, are also not authorized for use within or to the CBP trusted network.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.1.a	Data communication connections via modems are limited and tightly controlled as such connections can be used to circumvent security controls intended to protect CBP networks. Data communication connections are not allowed unless they have been authorized by the CISO. Approved remote access to DHS networks are only accomplished through equipment specifically approved for that purpose. Tethering with wireless mobile devices is prohibited unless approved by the appropriate AO.	AC-17
5.4.1.b	CBP centrally manages all remote access and dial-in connections to their systems to ensure integrity of network security. CBP also ensures that remote access and approved dial-in capabilities provide strong two-factor authentication, access control, audit capabilities, and protection for sensitive information throughout transmission. Remote access solutions comply with the encryption requirements of FIPS 140-2, *Security Requirements for Cryptographic Modules*. See Section 3.16, *Privacy and Data Security for additional information*.	AC-4 AC-17 AU-2 SC-7 SC-8
5.4.1.c	Remote access of PII complies with all CBP requirements for sensitive systems, including strong authentication. Strong authentication is accomplished via Virtual Private Network (VPN) or equivalent encryption and two-factor authentication. CBP has an immediate goal that remote access should only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. Any two-factor authentication is based on CBP-controlled certificates or hardware tokens issued directly to each authorized user.	AC-4 AC-17 AU-2 SC-7 SC-8

Policy ID	CBP Policy Statements	Relevant Controls
5.4.1.d	Remote access of PII do not permit the download and remote storage of information unless the requirements for the use of removable media with sensitive information have been addressed. All downloads follow the concept of least privilege and are documented with the SP.	---
5.4.1.e	CBP systems are not connected to any non-CBP systems via modem.	AC-17 AC-20
5.4.1.f	The Public Switched Telephone Network (PSTN) is not connected to OneNet at any time.	---
5.4.1.g	The Risk Assessment and SP documents any remote access of PII, and the remote access is approved by the CISO, CBP Privacy Officer, and AO prior to implementation.	AC-4 AC-17 AU-2 SC-7 SC-8

The following security policies apply to the approved use of modems in CBP-owned computers operating within or interfacing with non-CBP-owned systems and environments:

Policy ID	CBP Modem Policy Statements	Relevant Controls
5.4.1.h	For all dial-up connections, use a CBP-approved session-level encryption mechanism such as a smartcard, designed to protect both the identification and authentication process as well as data transmission. Unencrypted legacy dial-up systems, if in existence, is replaced.	AC-17
5.4.1.i	Workstations that have a physical connection to any network, mainframe, server, or other CBP device is not used to dial-up to non-CBP systems, unless such a dial-up is performed through a secured modem-pool authorized in writing by the CISO.	AC-17
5.4.1.j	If a requirement exists to use an on-board modem for dial-up capability, only a standalone workstation that does not contain sensitive information and that will never be physically connected to any other CBP system or network may be used.	AC-17
5.4.1.k	When located at an external site, standalone systems with their own dial-out capability to a CBP system require an ISA authorizing an interconnection. An ISA template is available from the DHS Information Assurance Compliance System (IACS). Contact your system's ISSO for details and assistance in obtaining the template.	AC-17

Remote access and dial-in responsibilities are provided below:

Remote Access and Dial-In Responsibilities
CISO • Establish and enforce remote access control policy for CBP. • Provide technical expertise and evaluate the effectiveness of remote access control approaches. **System/Network/LAN Administrators/FTOs** • Ensure that remote access controls are in place and functioning as intended. • Ensure that remote access controls provide strong identification and authentication. **ISSOs** • Ensure that remote access controls are in place and functioning as intended. • Ensure that remote access controls provide the security features outlined in this document. **Users** • When remotely accessing DHS systems, ensure that the equipment used to gain access is protected from viruses and other malicious code and that the protection software is kept current.

Unauthorized access is the biggest risk associated with remote access facilities. If untrusted or un-cleared persons obtain unauthorized access, they can violate the integrity, confidentiality, and availability standards of CBP. An unsecured modem or other dial-in facility could provide a backdoor for unauthorized users (inside or outside of CBP) to the entire CBP network. Malicious individuals can exploit improperly configured remote control software.

There are commercially available products that can be used in conjunction with other network protection mechanisms to reduce the risks of unauthorized access. These require the use of authentication methods stronger than passwords and user IDs. Only approved hardware and software products already contained within the Technical Review Model (TRM) can be purchased and operated without the need for additional approval of the CBP Architecture review function.

5.4.2 Network Security Monitoring

Security monitoring, detection and analysis are key functions and are critical to maintaining the security of CBP information systems. Network monitoring and analysis is limited to observing network activity for anomalies, malicious activities and threat profiles. Content analysis is not within the scope of network monitoring.

SOC leads the effort in monitoring network security. CISO, ISSOs, and system/network/LAN administrators/FTOs respond to and participate in intrusion alerts and SOC-led incident response investigations. They also evaluate the impact of each event on the system and implement any necessary corrections.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.2.a	The CBP SOC provides continuous monitoring of their networks for security events or outsource this requirement to the DHS ESOC. Monitoring includes interception and disclosure as required for the rendition of service or to protect the Department's or CBP's rights or property as well as properly identified and categorized information of third parties when required by the Department or CBP. In this instance, "rights" refers to ownership or entitlements or property or information as in intellectual property. Service observation or random monitoring is not used except for mechanical or service quality control checks. (As per the Electronic Communications Privacy Act)	SI-4
5.4.2.b	CBP SOC administers and monitors CBP Intrusion Detection System (IDS) sensors and security devices.	SI-4
5.4.2.c	CBP establishes monitoring scope at least as comprehensive and stringent as described in DHS 4300A Attachment F, *Incident Response.*	
5.4.2.d	The CBP SOC reports any event that is a security incident to the DHS ESOC.	SI-4

Network security monitoring responsibilities are provided below:

Network Security Monitoring Responsibilities
CISO • Establish policy and implement and manage a viable intrusion detection program within CBP. • Provide guidance, as needed, when responding to intrusion alerts from the DHS and/or CBP SOC. **SOC** • Monitor CBP systems and networks using various network security technologies. • Initiate computer security incident procedures when incidents are discovered. **ISSOs/System Administrators** • Respond to intrusion alerts when notified by DHS and/or CBP SOC. • Participate in SOC-led incident response investigations. • Evaluate the impact of the event on the system.

Network Security Monitoring Responsibilities
• Implement necessary corrective actions.

5.4.2.1 What Is Intrusion Detection?

Intrusion detection is the art of detecting inappropriate, incorrect, or malicious activity. Systems that operate on a host to detect malicious activity on that host are called Host-based Intrusion Detection Systems (HIDS). Those that operate on a network are referred to as Network Intrusion Detection Systems (NIDS). Intrusion detection is viewed as an integral part of a layered security model/defense-in-depth strategy.

Intrusion detection operates on the principle that any attempt to penetrate a system can be detected in real time as opposed to actually stopping the penetration, as is the case with firewalls. This principle is based on the assumption that it is virtually impossible to close every potential security breach. NIDS are designed to identify break-in attempts and stop them, in some cases working in conjunction with firewalls to alter the access control lists to halt an incursion. HIDS can offer the equivalent of a software firewall installed on the host, stopping or preventing would-be intruders.

Intrusion Prevention Systems (IPSs) are closely related to IDSs. Some IDS technologies currently provide intrusion protection by halting malicious data transmissions and disconnecting communication from the host from which they originate. Others take the additional step of reconfiguring firewalls to permanently block attacking hosts from sending data into the network.

Firewalls are designed to prevent unauthorized entry, but firewalls can fail or be compromised by an intruder. IDS supplement firewalls by alerting the organization that an attack may have occurred or be occurring. Firewalls are also incapable of protecting a network from internal compromise, but IDSs can alert network and system managers of such an attack.

5.4.2.2 Methods and Techniques

The most common approaches to intrusion detection are statistical anomaly detection and pattern matching (signature) detection.

Statistical anomaly involves tracking system use and establishing a baseline of what is “normal” and setting an acceptable range of parameters to which the system normally adheres. When the system goes beyond the statistical ranges, an intrusion may have occurred, and an alarm is given.

Pattern matching is simply what its name implies. Patterns of known attacks are part of the IDS database. Attack patterns for denial-of-service attacks, buffer overflow attacks, and backdoors are well known. These are known as signatures. When these signatures are detected, an alarm is given.

When alarms are given, those monitoring the IDS investigate to determine if an intrusion has in fact occurred and react accordingly. Event correlation systems can compare information from various security devices and reduce the likelihood of unnecessary response to “false positives,” which may arise from an attack signature matching allowed activities. Such systems can also

reduce the likelihood that the monitoring staff is distracted from noticing an actual attack by a flurry of alarms raised by relatively innocuous activities.

5.4.2.3 Network Monitoring

The SOC shall accomplish the monitoring of CBP systems and networks. Upon receipt of an alarm, operators shall investigate to determine the validity of the alarm. Once confirmed, the operator shall notify the ISSO and/or the system administrator for corrective action. If the problem is deemed critical, senior management shall be notified and involved to determine the appropriate course of action.

5.4.3 Network Connectivity

A system interconnection is the direct connection of two or more information systems for the purpose of sharing data and other information resources by passing data between each other via a direct system-to-system interface without human intervention. Any physical connection that allows other systems to share data (pass thru) also constitutes an interconnection, even if the two systems connected do not share data between them. System interconnections include connections that are permanent in nature, connections that are established by automated scripts at prescribed intervals, and/or connections which utilize Web and Service Oriented Architecture (SOA) services. System interconnections do not include instances of a user logging on to add or retrieve data, nor users accessing Web-enabled applications through a browser. External connections are defined as system(s) or IP addressable end points that are not under the direct control of DHS, systems that have IP addressing not in the DHS addressing scheme (routable and non-routable), or systems that have an authorizing official who is not a DHS employee.

Use Internet Protocol version 6 (IPv6) has been mandated by the Office of Management and IPv6, it is recommended that CBP ensure new technology acquisitions are able to send and receive IPv6 traffic, either through internal testing, or validated against a reputable organization, such as the U.S. Government version 6 (USGv6) Profile and Testing Program.

A number of management, operational, and technical controls impact network connectivity. These include identification and authentication controls, audit logging, integrity controls, and periodic reviews of programs/systems to ascertain whether or not changes that could adversely affect security have occurred.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.3.a	CBP ensures that appropriate identification and authentication controls, audit logging, and access controls are implemented on every network component/element.	AC-1 AC-2 AU-1 AU-2 IA-1 IA-2
5.4.3.b	Interconnections between CBP and non-CBP systems are established	CA-3

Policy ID	CBP Policy Statements	Relevant Controls
	only through the Trusted Internet Connection (TIC) approved service providers. The controlled interfaces are authorized at the highest security level of information on the network. Connections with other Federal agencies are documented based on interagency agreements, Memoranda of Understanding (MOU), Service Level Agreements (SLAs) or Interconnection Security Agreements (ISA). The document vehicle chosen contains such information as the interface characteristics, security requirements, nature of information communicated and monitoring procedures for verifying enforcement of security requirements.	
5.4.3.c	CBP documents all interconnections to the DHS OneNetwork (OneNet) with an ISA, signed by the OneNet AO and by the CBP AO. See Attachment N, *Preparation of Interconnection Security Agreements* and Section 5.4.3.1, *Interconnection Security Agreements* for more details on ISAs.	CA-3
5.4.3.d	ISAs are reissued every three (3) years or whenever any significant changes have been made to any of the interconnected systems.	CA-3
5.4.3.e	ISAs are reviewed and updated as needed as a part of the annual Federal Information Security Modernization Act of 2014 (FISMA) self-assessment.	CA-3
5.4.3.f	CBP may complete a master ISA, (which includes all transitioning systems) as part of their initial OneNet transition. After transition, each additional system or General Support System (GSS) is required to have a separate ISA. Interconnections between CBP and other DHS Components (not including DHS OneNet) require an ISA whenever there is a difference in the security categorizations for confidentiality, integrity, and availability between the systems or when the systems do not share the same security policies. In this context, 'security policies' refers to the set of rules that controls a system's working environment and not to DHS information security policy. ISAs are signed by each organization's respective AO.	---
5.4.3.g	CBP documents interconnections between the CBP network and external (non-DHS) networks with an ISA for each connection.	CA-3
5.4.3.h	A single ISA may be used for multiple connections provided that the security authorization is the same for all connections covered by that ISA.	CA-3
5.4.3.i	CBP implements a Trust Zone with DHS through Policy Enforcement Points (PEP), as defined in the DHS Security Architecture and documented in Section 5.4.3.2, *Trust Zones*.	SC-7
5.4.3.j	DHS OneNet provides secure Name/Address resolution service.	SC-20

Policy ID	CBP Policy Statements	Relevant Controls
	Domain Name System Security Extensions (DNSSEC) has been designated as the DHS service solution.	SC-21 SC-a
5.4.3.k	All DHS systems connected to OneNet and operating at moderate or high level utilize secure Name/Address resolution service provided by DHS OneNet.	SC-20 SC-21 SC-22
5.4.3.l	The appropriate Change Control Board (CCB) ensures that documentation associated with an approved change to an information system is updated to reflect the appropriate baseline. CBP systems that interface with OneNet are also subject to the OneNet CCB.	CM-3
5.4.3.m	Interconnections between two authorized DHS systems do not require an ISA if the interface characteristics, security requirements, nature of information communicated and monitoring procedures for verifying enforcement of security requirements are accounted for in the Security Plans (SPs) or are described in another formal document, such as an SLA or contract, and the risks have been assessed and accepted by all involved AOs.	CA-3
5.4.3.n	Granting the ability to log into one DHS system through another DHS system (such as through OneNet trust) does not require an ISA, when the requirements from Policy Section 5.4.3.m above are met.	---
5.4.3.o	The information system protects the authenticity of communications.	SC-23
5.4.3.p	For systems with high or moderate impact for any of the FIPS 199 security objectives, system resource sharing is limited to an operational need. The information system prevents unauthorized and unintended information transfer via shared system resources. All information transfer is limited to that information which has been included in the security plan and has been analyzed in the risk assessment for the system.	SC-4

Network connectivity responsibilities are provided below:

Network Connectivity Responsibilities
CISO • Provide guidance and enforce management, operational, and technical controls that apply to network and system security configuration and monitoring. • Evaluate the risks associated with external connections. • Review programs/systems periodically to ascertain if changes have occurred that could adversely affect security. **AO or Designated Official** • Review, approve, and sign the ISA. • Ensure that ISAs are reissued every three years or whenever significant changes are made to any of the interconnected systems. **System Owners** • Establish the requirement for the external connection and assess the associated risks. • Ensure that all connections to the system are identified and addressed by an active ISA document. **Network Administrators** • Ensure technical controls governing use of the external connection remain in place and function properly. • Assist in development of the ISA as necessary. • Ensure that any new connection and/or system access was justified and validated by the system owner and the system ISSO. • Ensure that there is a valid ISA in place prior to any connection being activated. **Certifying Agents** • Review Mission ISAs developed by the ISSOs before the ISA is sent for signature approval. **ISSOs** • Coordinate with the external agency in development of the ISA. • Ensure that a validated list of connections and supporting ISAs is included in the Security Plan and is also available as necessary by CISO in support of Secure Internet Gateway (SIG) requests. • Assist in preparation of both Trade and Mission ISAs and ensure all external connections

Network Connectivity Responsibilities
are documented in the Security Plan, Risk Assessment, and security operating procedures. • Review ISAs as a part of the annual FISMA self-assessment. • Monitor compliance. **Users** • When connecting to CBP networks, ensure the equipment used to access these networks is protected from viruses and other malicious code and the protection software is kept current.

5.4.3.1 Interconnection Security Agreements

Proper management of network connections is vital to ensuring the confidentiality, integrity, and availability of the data processed by a system. Interconnections of systems must be established in accordance with NIST SP 800-47 (*Security Guide for Interconnecting Information Technology Systems*).

An ISA is required whenever the security policies of the interconnected systems are not identical, or the systems are not administered by the same entity. The ISA documents the security protections on the interconnected systems to ensure only acceptable transactions are permitted. ISAs must be reissued every three years or whenever significant changes have been made to any of the interconnected systems. CBP ISSOs must review their ISAs as part of the annual FISMA self-assessment.

All external connections must be identified and documented in the Security Plan, the risk assessment, and other Security Authorization documentation as necessary. The risk associated with these connections must be addressed during the Security Authorization process.

An ISA should address the following areas:

1. Purpose: This section should explain the rationale for the interconnection and contain a one- or two-paragraph statement that justifies the need to interconnect the two systems.

2. Interconnection Statement of Requirements: This section documents the formal requirement for connecting the two systems. The following items should be addressed in this section:

    a. The requirement for the interconnection, including the benefits derived

    b. The names of the systems being interconnected

    c. The type of connection (Frame Relay, T1, etc.)

    d. Physical location of connection equipment, including addresses and room numbers

e. Primary Points of Contact (POC) for both systems

f. The agency name(s) or organization that initiated the requirement

3. System Security Considerations: This section documents the security features in place to protect the confidentiality, integrity, and availability of the data and the systems being interconnected. This includes such areas as incident reporting and personnel clearances. Technical representatives from each organization need to discuss the contents of this section and come to a mutual agreement as to which items will be included.

4. Topological Drawing: Each ISA must include a topological drawing depicting the end-to-end interconnectivity in a clear and readable manner. The drawing should include:

   a. All data communications paths (not program system paths), circuits, etc., used for the interconnection beginning with the DHS-owned system(s) traversing through all interconnected systems to the non-DHS endpoint.

   b. The logical location of all components (mainframe computers, host processors, hubs, firewalls, encryption devices, routers, frame relay devices, Secure Frame Units (SFU), Communications Service Units (CSU), Data Service Units (DSU), and customer personal computers).

5. Signatures and Comments: Each ISA must be signed by the CBP AO of each connecting system and/or organization or by the official designated by the AO to have signatory authority for ISAs. This section acknowledges that the ISA is subject to change, will be reviewed annually, and will be modified as circumstances warrant. This section must include a statement that the ISA may not be unilaterally modified and that any changes must be reviewed and jointly agreed upon.

Details on completing an ISA are contained in 4300A Attachment N, *Preparation of Interconnection Security Agreements*.

5.4.3.2 Trust Zones

Information and services sharing between the DHS ESOC and CBP occurs through Trust Zones. A Trust Zone consists of a group of people, data systems, and networks subject to a shared security policy or set of rules governing access to data and services. (For example, a Trust Zone may be set up between different network segments that require specific usage policies based on information processed, such as law enforcement information.) The DHS ESOC must be aware of CBP-security requirements, as defined by Trust Zones, to accurately perform DHS ESOC duties.

DHS Trust Zones have the following characteristics:

1. The Trust Zone must be set of networked hosts protected from unconstrained access by one or more security perimeter devices

2. There must be a basis for placement and configuration of firewalls, Virtual Private Networks (VPN), and remote access protection devices

3. The Trust Zone may consist of a single host, one or more Local Area Networks (LANs) at a site, or a group of networks connected via a network provider or backbone

4. OneNet provides a layer of trust through subnetting, firewalls, and other policy enforcement mechanisms

5. Network Admission Control permits dynamic assignment of information systems and users to basic Trust Zones. Medium and High assurance models are another mechanism that permits assignment to Trust Zones

Application based Trust Zones permit organization managed Trust Zones.

5.4.3.3 Domain Membership

This policy is required to improve the manageability and security of Windows desktops and devices connected to the network. Adherence to this policy shall ensure that CBP is in a position to detect and remediate vulnerable windows systems. Workstations are the largest attack surface within DHS and require many controls to ensure they are properly managed. This has become even more critical in the wake of recent attacks, as unmanaged systems are easy to exploit via well-known avenues. These exploits have subsequently caused significant disruption to the CBP mission.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.3.3.a	All computers and mobile devices running a Microsoft Windows operating system connecting to CBP's Networks are required to join one of the five managed Windows Domains, which are listed as follows: 1.) CBP Development Domain: DEV.CBP.DHS.GOV 2.) CBP Quality Assurance Domain: QAX.CBP.DHS.GOV 3.) CBP Production Domain: AD.CBP.DHS.GOV 4.) CBP Application Domain: APP.AD.CBP.DHS.GOV 5.) CBP DMZ Domain: PAD.CBP.DHS.GOV	---
5.4.3.3.b	Only "approved" CBP Windows (Workstations/Servers) versions are permitted. Please note that the requirement to join one of the CBP managed domains does not grant approval for unauthorized operating systems, software or configuration therein.	---
5.4.3.3.c	All computers and mobile devices that are members of the Active Directory Windows Domain have the 'Domain Admins' group as a member of the local Administrators group. When Windows computers join the domain, this group is automatically added, and it is not removed.	---

Policy ID	CBP Policy Statements	Relevant Controls
5.4.3.3.d	In cases where computers and mobile devices do not require access to central resources such as file or print servers, e-mail or Internet access, then an exemption to domain membership is sought through the assigned ISSO and/or STP. Such an exemption would be conditional upon the department involved accepting responsibility for maintaining adequate patching and virus protection levels. Exemptions may also be conditional upon the limitation of network access to the non-domain computer equipment.	---
5.4.3.3.e	Non-CBP equipment that cannot join the Active Directory Windows domain is subject to a separate Waiver covering the responsibilities of the department or owner. This level of access is required in order to verify service pack and patch levels, virus definitions, software versions and (where necessary) to purge or remove virus infections.	---

5.4.4 Firewalls and Policy Enforcement Points

Policy Enforcement Points (PEPs) separate Trust Zones as defined by the DHS Security Architecture. Boundary protection between DHS and external networks is implemented by firewalls at Trusted Internet Connections (TICs) and other approved direct system inter-connections. DHS TICs are provided by OneNet and monitored by the DHS ESOC. CBP SOC may protect CBP boundaries across the DHS Trust Zones.

Within CBP, boundary protection of IT resources is accomplished by the installation and operation of firewall systems. Firewalls, when used in concert with a variety of additional security controls such as Intrusion Detection Systems (IDS), personnel background checks, security guards, data encryption, and physical security barriers, provide an added level of assurance that unauthorized personnel will be unable to access CBP's automated systems.

By tracking and controlling data, and deciding whether or not to pass, drop, reject, or encrypt the data, firewalls have proven to be an effective means of securing a network.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.4.a	CBP restricts physical access to firewalls and PEPs to authorized personnel and ensures that all firewalls are located only in a physically secure area.	AC-4 SC-7
5.4.4.b	CBP implements identification and strong authentication for administration of the firewalls and PEPs.	
5.4.4.c	CBP encrypts remote maintenance paths to the firewalls and PEPs.	MA-4 SC-7
5.4.4.d	CBP conducts quarterly firewall and PEP testing to ensure that the most recent policy changes have been implemented and that *all* applied policies and controls are operating as intended.	SC-7
5.4.4.e	CBP SOC ensures that reports on information security operations status and incident reporting are provided to the CISO as required by this	IR-6

Policy ID	CBP Policy Statements	Relevant Controls
	Policy Directive.	
5.4.4.f	All Department and CBP firewalls and PEPs are administered in coordination with DHS security operation capabilities, through the DHS ESOC or CBP SOC.	SC-7
5.4.4.g	All DHS PEPs provide protection against denial-of-service attacks.	SC-5
5.4.4.h	CBP determines protocols and services permitted through the CBP PEPs. CBP may restrict traffic sources and destinations at the CBP-level PEPs.	SC-7
5.4.4.i	The DHS ESOC oversees all enterprise PEPs, including the CBP PEPs.	---
5.4.4.j	CBP ensures each information system separates user functionality (including user interface services) from information system management functionality. User interface services (e.g., public web pages) are separated physically and logically from information storage and management services (e.g., database management). The separation may be accomplished through the use of different computers, different central processing units, different instances of operating systems, different network addresses, or a combination of these or other techniques. (Isolation of a public web page in a Demilitarized Zone (DMZ) is an example of this separation.)	SC-2 SC-32
5.4.4.k	For high impact systems, the information system isolates security functions from other functions.	SC-3
5.4.4.l	For high impact systems, the information system fails to a known state while preserving system state information in failure.	SC-24
5.4.4.m	For high impact systems, the information system: a) Verifies the correct operation of related security functions b) Performs this verification upon reboot, or command by user with appropriate privilege c) Notifies an authorized person of failed security verification tests d) Provides a CBP-defined action when anomalies are discovered (e.g., shuts the information system down or restarts the information system).	SI-6
5.4.4.n	Certification and/or security authorization in accordance with the procedures established in this handbook.	CA-2
5.4.4.o	Configured to prohibit any protocol or service that is not explicitly permitted by CBP LAN standards and security certified configurations.	AC-6 CM-3 CM-7
5.4.4.p	The DHS ESOC provides a central coordination and reporting point to integrate the efforts of CBP and other component SOCs (including the Homeland Security Secure Data Network (HSDN) SOC), creating a "community of the whole." While SOCs are localized, specialized, and operational within each Component, the central reporting structure	PM-1

Policy ID	CBP Policy Statements	Relevant Controls
	enables Department-wide coordination and collaboration.	
5.4.4.q	Audit capabilities of the system are enabled to collect the following information, at a minimum: • Source and destination Internet Protocol (IP) address • Time and date of event • Uniform Resource Locator (URL) • Access attempts to network services • Rejected source-routed addresses • Use of Internet Control Message Protocol (ICMP) • Redirects	AU-2
5.4.4.s	Provide intrusion detection capability, either as an integral part of the firewall or through a separate, add-on appliance. The IDS provides for a scalable response to attacks and remote notification.	AC-6 IR-4 SI-4
5.4.4.t	The System Administrator (SA) for any CBP-owned firewall or server accessible from the Internet or an Extranet should not be the same person that is the SA for the internal system or network connected to the Internet or the Extranet by the firewall or server.	AC-5
5.4.4.u	The transmission of CBP-owned, non-public information from a CBP server over private networks, the Internet, or Extranet to any user uses a secure protocol that provides FIPS 140-2 compliant cryptographic protection.	SC-13
5.4.4.v	Any CBP-owned firewall or server for which Internet or Extranet connectivity is approved prohibits the login of a SA from the Internet or Extranet.	SC-11
5.4.4.w	Any CBP-owned firewall or server accessible from the Internet or an Extranet provides an intrusion detection capability that provides an immediate alert when an attack or attempt to bypass system security occurs.	SI-4 SI-5
5.4.4.x	Any CBP-owned firewall or server accessible from the Internet or an Extranet maintains audit records of all transactions, and such records are stored on tamper-proof media or routed to a host that is not accessible from the Internet or Extranet.	AU-9
5.4.4.y	The operating system and all associated software of any CBP-owned firewall or server accessible from the Internet or any Extranet are kept current with respect to security-related patches, modifications, fixes, etc. Patch updates follow the guideline set forth within the ISVM notice published by DHS-SOC. The Change Control Board (CCB) prior to deployment approves all patches. In the case of emergency patches to mitigate a known, immediate threat to the CBP network, the CCB may be bypassed with written approval of the CISO.	CM-2 SI-2

Policy ID	CBP Policy Statements	Relevant Controls
5.4.4.z	The implementation and use of Common Gateway Interface (CGI) scripts on any firewall or server are monitored and controlled. Scripts do not allow users to activate command-level instructions or to perform any system administrator function. All scripts are limited to performing their functions from within their own directory with all Server Side Includes (SSIs) disabled.	SA-9

Responsibility for the future deployment and management of firewalls will be determined at a later date. General responsibilities are included below:

Firewall Responsibilities
CISO • Develop procedures and schedules for deploying firewall systems. **ISSOs and ADP Support Personnel** • Assist CBP teams in the installation and configuration of firewall systems. **Site Managers** • Ensure that the installation team receives necessary support during and after firewall installation. **SOC** • Manage firewalls in accordance with DHS and CBP firewall policies. • Maintain change control over firewalls and maintain proper firewall configuration. • Evaluate, process, and approve changes to firewall configuration.

5.4.4.1 Firewall Basics

A firewall is a system or group of systems that enforce an access control policy between two networks. The actual means by which this is accomplished varies widely. Associated with the basic capabilities of access control, firewalls can authenticate the source and destination of a given data path, provide Network Address Translation (NAT) and Port Address Translation (PAT) and log all traffic passing through them. The logging is either done on the machine on which the firewall software runs on or is logged to a separate machine for audit and intrusion forensic analysis.

Firewalls are often associated with filtering devices, which screen incoming (and possibly outgoing) data traffic for viruses and malware in the form of mobile code. By offloading these responsibilities to ancillary machines, the firewall can allow higher rates of data transmission.

Mobile (downloadable) code is software that is transmitted from a remote source across a network to a local system and then executed on that local system (e.g., personal computer, wireless mobile devices, Internet appliance). Examples include ActiveX controls, Java applets, script run within the browser, and HTML email. Although mobile code is a legitimate method for distributing application software, it is most frequently associated with "malicious mobile code" (e.g., viruses, worms, Trojan horses) that executes without the permission of or any explicit action by the local system's owner/user.

Firewalls also have two facets with respect to encryption. A frequently used mechanism is the SSHv2 protocol (Secure Shell version 2). This facility can provide for authentication by a digital certificate or a two-factor authentication mechanism, as well as strong encryption. Such a connection should only be allowed from the protected (internal) side of a firewall, so that unauthorized outsiders are unable to affect a change.

Firewalls often have the capability to implement encrypted data communications. Although this approach might be slightly more economical, it is more prudent to have a system that functions as a firewall serve a single purpose. A separate encryption server (behind the firewall) is afforded the extra protection of being shielded by a firewall. Encryption, moreover, involves a substantial amount of computational power, which would slow down the operation of the firewall. Lastly, if the firewall system is compromised, the encryption facility is not automatically compromised at the same time.

National Institute of Standards and Technology (NIST) SP 800-10, *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls*, and NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy,* offer guidance with respect to firewalls and the functions they can serve.

5.4.4.2 Firewall Deployment

Firewall systems have been deployed to various CBP sites, and additional systems are scheduled for deployment as part of the continuing effort to provide necessary security safeguards.

Firewalls are not used solely to provide boundary protection from the outside world. In commercial environments, for example, the fiscal processing systems may be protected from the remainder of the network by firewalls. In a similar manner, CBP can use firewalls to segment systems that have various levels of sensitivity, unless they are so classified that connection to the network should be prohibited.

5.4.4.3 Firewall Management

All firewalls for unclassified and collateral classified systems shall be under the control of the DHS and CBP SOCs, who are responsible for providing direction and guidance for firewall settings and rule sets. The actual application of all firewalls shall be under the DHS ESOC.

5.4.4.4 Unauthorized Firewall Protocols and Services

All unused firewall and gateway ports will be disabled. Use of the following firewall protocols and services are unauthorized, and the associated ports will be disabled.

Table 5.4.4.4: Unauthorized Firewall Protocols and Services

Unauthorized Firewall Protocols and Services		
BFTP	NFS	RLP
Chargen	NNTP	SNMP*
Echo	POP	SunRPC
Finger	POP2	Supdup
Link	POP3	Syslog
LPD	Portmap	GOPHER
Name	RCF	UUCP
Netbios	RIP	X Protocols
ICMP Redirects	NIS	R Commands
UDP Boot Services	RIP Daemon, Routed	FTP
TelNet		

* Although SNMP is prohibited for use in external Internet facing network devices as stated in DHS IT Security Policy, properly configured SNMP may still be used in order to monitor and manage internal CBP computing devices. A secure version of SNMP is recommended with internal CBP network devices configured following the hardening guidance.

Use of any unauthorized service must have formal approval of the AO. A waiver or exception must be obtained before implementing any of these services. Approval may not be granted unless it can be demonstrated that the selected firewall configuration provides adequate security in accordance with CBP Security Authorization security requirements and CBP system hardening guidance in accordance with CBP-developed protection profiles.

5.4.4.5 Authorized Protocols and Services

Secure protocols and services, such as SSH, Secure File Transfer Protocol (SFTP), and Transport Layer Security (TLS) may be permitted where it can be demonstrated that they do not negatively impact the security of network operations or other interconnecting systems. Hardening guidelines must be followed for implementation and maintenance of such systems. Use of such protocols or services must be approved by the AO and fully documented in Security Authorization documentation of systems employing these technologies.

5.4.4.6 Virtual Private Network Personal Firewalls

CBP-owned laptops or desktops requiring broadband connections must be equipped with a CBP-approved personal firewall. The required security configuration of the personal firewall must include the following features:

1. The personal firewall shall block externally originated incoming network requests. An exception is permitted for TIVOLI and CBP trusted security-monitoring systems.
2. Users will not have the capability to disable the personal firewall. Any command line scripts associated with firewall activity shall be hidden from user view or access.
3. The personal firewall shall be used with and within the DHS/CBP trusted networks.
4. An outgoing Virtual Private Network (VPN) connection is only permitted via personal firewall. Incoming broadband connections to the host are permitted only through a VPN tunnel.
5. Personal firewall outgoing, IP-initiated communications shall be permitted only to DHS/CBP trusted sub-nets. An exception is permitted for Dynamic Host Configuration (DHCP)-initiated requests required to establish the VPN tunnel.
6. The personal firewall must operate with CBP network firewall systems.
7. The personal firewall shall not allow users to initiate communications directly to the Internet. All Internet communications, if any, shall be established through direct connection with the LAN at a DHS/CBP trusted site or through the CBP VPN.
8. The personal firewall is required for the broadband VPN overlay product on the certified CBP Standard Desktop Operating System.
9. The personal firewall will be initiated when the desktop or laptop system is powered on and remain on until the system is powered off.
10. CBP systems using broadband VPN must be configured to automatically disable any capability to bridge traffic from other network connections via modem or wireless access points. Users must not have the capability to change this configuration.

5.4.4.7 Firewall Exceptions and Waivers

Exceptions and waivers for CBP firewall policy and the configuration requirements in this section require formal written requests to and approval from the CBP AO and the CISO prior to changing currently authorized configurations to operate unauthorized ports and services. Any such changes to approved configurations must be fully documented.

Requests for an exception or waiver must be first submitted to the CISO and must provide the following information:

1. A description of the desired exception and waiver
2. A detailed business case to justify use of the unauthorized service
3. A risk assessment associated with implementing the service
4. Actions taken to mitigate identified risks

Exceptions or waivers that have been approved by the CBP AO must be included in an updated security authorization package reflecting the new services and their associated risks. New services must not become operational until the CBP AO has re-approved the system and granted Approval-To-Operate (ATO) with use of those services.

5.4.5 Router Device Management

The following practices should be followed in order to maintain the security posture and availability of the CBP networking devices:

1. Communications between devices must be secured by restricting communication to known authorized IP addresses at a minimum.
2. All network management ports must be disabled except those needed to support the operational commitments of the site.
3. The router administrator will manage devices through out-of-band or direct connection. If out-of-band management is not feasible, the use of "in-band" management will be limited to situations where the use of out-of-band management would hinder operational commitments or in an emergency situation. The CISO will approve the use of "in-band" management on a case-by-case documented basis.
4. All security-related patches applied for out-of-band access will use the currently supported version of SSH.
5. Where management of remote site devices is impractical using the direct connection method, secure dial-up method via an encryption utility is acceptable. Termination of the secure dial-up must be at the Terminal Access Controller Access Control System+ (TACACS+) server inside the secure enclave.
6. Authenticated access control using out-of-band management must be used for access via remote access devices. This will be enforced with strong two-factor authentication, encryption of management session, and auditing. This method ensures only authorized network administrator access via remote devices.
7. Due to bandwidth limitations, use of "in-band" management will be restricted to a limited number (less than 10) of authorized IP addresses, including the SA and his backup. This may be accomplished through the vendor's Network Management System (NMS) or by using an access control list.
8. In-band connections will use strong two-factor authentication for all managed communications devices.
9. Where port management and port protection services are available on communication devices, they will be activated on all authorized port connections.

10. Banners warning users that their computer activity may be monitored must be displayed on all network management devices allowing Hyper-Text Transfer Protocol (HTTP) access. All devices that do not support warning banners must be documented.

5.4.6 Internet Security

Over the past few years, government, private industry, and academia have developed security techniques, practices, and tools to reduce the ever-growing risks associated with interconnected networks. The policy contained in this section establishes minimum-security requirements to connect CBP information systems with the Internet, the CBP Intranet, and any Extranet. In some cases, business needs will determine the necessity of more stringent connectivity requirements.

Any CBP-owned Internet Web site providing public information, regardless of the ownership of the service provider, must conspicuously display the Security Notification, documented in Section 5.2.3**,** *Warning Banner* either in full text on the first page or with a button containing the words "Legal & Privacy Notices" located conspicuously on the first page.

This section provides specific CBP technical policy regarding the use and proper configuration of firewalls and the management of dial-up connections and other protocols.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.6.a	Any direct connection of CBP networks to the Internet or to extranets occur through firewalls and CBP TIC PEPs that have been authorized.	SC-7
5.4.6.b	Firewalls and PEPs are configured to prohibit any protocol or service that is not explicitly permitted.	CM-7 SC-7 SC-8
5.4.6.c	CBP ensures that all executable code, including mobile code (e.g., ActiveX, JavaScript), is reviewed and approved by an appropriate senior official prior to the code being allowed to execute within the CBP environment. Note: When the technology becomes available and code can be vetted for security, the policy will be "Ensure that all approved code, including mobile code (e.g., ActiveX, JavaScript), is digitally signed by the designated CBP authority and that only signed code is allowed to execute on CBP IT systems."	SC-18
5.4.6.d	Telnet is not used to connect to any CBP computer. A connection protocol such as Secure Shell (SSH) that employs secure authentication (two factor, encrypted, key exchange, etc.) and is approved by CBP is used instead.	CM-7 SC-7 SC-8
5.4.6.e	File Transfer Protocol (FTP) is not used to connect to or from any CBP computer. A connection protocol that employs secure authentication (two factor, encrypted, key exchange, etc.) and is approved is used instead.	CM-7 SC-7 SC-8
5.4.6.f	Remote Desktop connections, such as Microsoft's Remote Desktop Protocol (RDP), is not used to connect to or from any CBP computer	AC-17 IA-2

Policy ID	CBP Policy Statements	Relevant Controls
	without the use of an authentication method that employs secure authentication (two-factor, encrypted, key exchange, etc.).	
5.4.6.g	To ensure the security and availability of CBP information and information systems the CBP CIO or CISO may direct that specific Internet websites or categories be blocked at the CBP Trusted Internet Connections (TIC) as advised by CISA, the DHS and CBP SOCs, or other reputable sources.	---
5.4.6.h	All users accessing Internet HTTP sites use a CBP-approved available HTTP browser. Such browsers incorporate all vendor-provided security patches, modifications, fixes, etc. Patch updates follow the guideline set forth within the ISVM notice published by DHS-SOC. All HTTP browsers are configured securely according to CBP security standards set by the CISO. Security settings on HTTP browsers are not to be modified by CBP users at any time for any reason.	SC-7
5.4.6.i	All files obtained from the Internet, or an Extranet are scanned upon receipt before they are opened or used. CBP-approved and properly updated anti-virus scanning and detection software is used.	SI-3
5.4.6.j	CBP-owned sensitive information is not stored on or distributed via publicly accessible Web hosting.	MP-1
5.4.6.k	Electronic mail traffic between the Internet and internal networks are implemented with centrally managed Simple Mail Transfer Protocol (SMTP) gateways.	AC-13
5.4.6.l	Proxy applications are used to route mail through firewalls.	AC-4
5.4.6.m	No CBP data (in any form including “mailbox” data, other than the account information necessary to operate the system) is located on application gateways or firewall devices.	AC-4
5.4.6.n	All network switch ports (i.e. network jacks) in public spaces such as primary and secondary inspection areas have security controls to prohibit unauthorized access.	PE-1 PE-2 PE-3 PE-7
5.4.6.o	Any CBP-owned Internet Web site providing public information, regardless of the ownership of the service provider, conspicuously displays the approved legal and privacy notices. It is displayed either in full text on the first page or with a button containing the words “Legal & Privacy Notices” located conspicuously on the first page. The accepted language is located on the DHS CISO site: https://usdhs.sharepoint.com/sites/dhsconnect/org/comp/mgmt/ocio/ciso/Pages/sspolicy.aspx	AC-8

Internet security responsibilities are provided below:

Internet Security Responsibilities

CBP AO
• Ensures all external network connections are protected by a firewall and possibly other boundary protection devices that have been authorized at a level commensurate with the sensitivity of the information to be protected.
• Ensures dial-up connections are addressed in the Security Authorization documentation.
ISSOs
• Ensure all external network connections are addressed in the risk assessment and Security Plan.
• Ensure all external network connections are protected by a firewall and possibly other boundary protection devices.
• Ensure all boundary protection devices are properly configured and monitored.
• Ensure dial-up connections are properly configured and secure.
Network/System Administrators/Field Technology Officers
• Ensure all boundary protection devices are properly configured and monitored.
• Ensure firewall ports that allow file and printer sharing, whether through Microsoft NetBIOS, Common Internet File Service (CIFS), Network File Services (NFS), or Transport Control Protocol (TCP) SMB (Server Message Block) protocols, are closed.
• Ensure firewalls are configured to prohibit any protocol or service that is not explicitly permitted.
• Ensure the following are prohibited:
  o Telnet (clear text) connections
  o File Transfer Protocol (FTP) unsecured (clear text) file transfers
  o Simple Network Management Protocol (SNMP) that can be used to monitor and control systems
  o Cross boundary routing broadcasts
  o Address Resolution Protocol (ARP) messages
  o Domain Name System (DNS) communications across the boundary (by using split DNS with zone transfer authentication)
  o Unsecured file transfers
  o Mobile code (e.g., ActiveX, JavaScript) that has not been reviewed and digitally signed by an appropriate DHS authority.
• Ensure dial-up connections are properly configured and secure.

Sound network security practice dictates that all network connections are identified, and the threats and vulnerabilities associated with these connections be analyzed. The guidance provided in Section 5.4, *Network and Communications Security*, specifically with regard to Interconnection Security Agreements (ISAs), also applies to connections to Internet and extranet connections. An *extranet* is a private network encompassing that portion of an organization's intranet that it chooses to securely share—via the Internet and the public telecommunication system—with external suppliers, vendors, or customers. An extranet requires security and privacy and may involve firewalls, digital certificates, message encryption, and VPNs that can tunnel through the public network.

All external connections, including extranets, must be identified and documented in the Security Plan, the risk assessment, and other Security Authorization documentation as necessary. The risks associated with these connections must be addressed during the Security Authorization process. Additionally, external network connections are to be reviewed annually by ISSO and documented in the annual information security assessment.

Adequate protection requires the proper selection and installation of firewalls and other boundary devices, Intrusion Detection Systems, and ancillary encryption or filtering devices. These devices must be authorized prior to their use on DHS networks. Implementation guidance for firewalls is discussed in Section 5.4.4, *Firewalls and Policy Enforcement Points*. Intrusion Detection Systems are covered in Section 5.4.2.1, *What is Intrusion Detection*? Also, see Section 5.7.1, *Encryption*. The adequacy of these devices must be monitored and reviewed as part of periodic information security assessments.

Firewalls must be configured to prohibit any Transport Control Protocol (TCP), User Datagram Protocol (UDP) service, or other protocol that is not explicitly permitted. Of particular concern is the need to close ports that allow file and printer sharing, whether through Microsoft NetBIOS, Common Internet File Service (CIFS), Network File Services (NFS), or TCP SMB protocols. The use of file and printer sharing is associated with numerous vulnerabilities related to everything from enumeration of devices and user accounts to anonymous control of systems without authorization.

Telnet, which is prohibited on CBP systems and networks, is a utility program and protocol that allows one computer to connect to another computer on a network. After providing a username and password to login to the remote computer, a user can enter commands that will be executed as if entered directly from the remote computer. Telnet transfers all information in "clear text" (human readable text), which allows Internet service providers (ISPs) and other users on the Internet, intranet, or LAN to intercept the traffic it creates. This could allow unauthorized users to get user IDs and passwords, capture information or commands that are being sent, and potentially alter the information in the telnet connection. Telnet uses a commonly known port, which makes it easy for someone to "sniff" telnet traffic. The approved solution for this functionality is to use SSH. SSH is an Internet Engineering Task Force (IETF) protocol that provides encrypted connections and supports authentication with digital certificates and other secure methods of authentication.

File Transfer Protocol (FTP) is a means of transferring files from one computer to another. FTP transfers all information in clear text (unencrypted human readable text), which allows Internet Service Providers (ISP) and other users on the Internet, intranet, or LAN to intercept the traffic it creates. This allows unauthorized users to capture information or commands and possibly alter the information in the FTP connection. FTP generally uses a commonly known port, which makes it easy for someone to "sniff" FTP traffic. The approved solution for this security risk is to use the Secure File Transfer Protocol (SFTP) component of SSH. SSH is a Federal Information Processing Standards (FIPS) 140-2-approved IETF protocol, which provides encrypted connections and supports authentication with digital certificates and other secure methods of authentication.
Use of the following is expressly prohibited:

- Telnet
- File Transfer Protocol (FTP)
- Simple Network Management Protocol (SNMP), which can be used to monitor and control systems
- Address Resolution Protocol (ARP) messages

The following have significant risks and shall be used only in conjunction with appropriate countermeasures and risk-reduction procedures:

- Cross boundary routing broadcasts
- Domain Name Service (DNS) communications across the boundary (by using split DNS with authentication of zone transfers)
- Mobile code (e.g., ActiveX, JavaScript) that has not been reviewed and digitally signed by an appropriate DHS authority

Implementation guidance for securing dial-up connections is addressed in Section 5.4.1, *Remote Access and Dial-In*. If a dial-in connection can be justified, it must be strictly controlled.

Securing Internet Connections

Internet connectivity exposes CBP systems to damage caused by adversaries exploiting CBP vulnerabilities (e.g., malicious code). In order to limit the risk, users at a minimum must follow the Rules of Behavior listed below:

1. CBP Internet connections are for official business and use of the Internet must be within the scope of duties of the individual unless access has been approved for Limited Personal Use. (See Section *Personal Use of Government Office Equipment and DHS IT Systems/Computers*).

2. CBP equipment capable of providing Internet connectivity will not be used for any activity that would adversely affect the confidence and public integrity of the CBP service, even when used for approved "Limited Personal Use."

3. STP reserves the right to review, audit, intercept, access, and disclose information on all Web sites visited by any user during his/her Internet connectivity. The page contents of Internet Web sites obtained for any purpose may be disclosed within the CBP domain without the permission of the employee. Supervisors are responsible for ensuring that employee use of CBP-owned office equipment for non-government purposes is in accordance with the CBP Limited Use Policy.

4. CBP sensitive information must not be transmitted via the Internet without using approved security controls, such as encryption, and obtaining authorization.

5. Users may accept session "cookies," which are small text files that some Web sites store on your hard drive temporarily. Government sites will provide clear and conspicuous notice that "cookies" are used, but these are deleted at the end of the session.

6. Browser configuration settings will not be set to accept permanent cookies unless explicitly approved for official purposes by the CISO.

7. The Internet should not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, CBP law enforcement data or similar materials without the express permission of the data owner. The confidentiality of Internet traffic is not guaranteed.

8. CBP users are not authorized to download copies of data or software systems from the Internet unless the activity is associated with an approved/official procurement process or approved by the CISO. All authorized downloads must be scanned for viral infection before installing the software.

9. Remote Desktop connections, such as Microsoft's Remote Desktop Protocol (RDP), shall not be used to connect to or from any DHS computer without the use of an authentication method that employs secure authentication (two-factor, encrypted, key exchange, etc.).

10. The following Internet, Intranet, and Extranet activities are unauthorized:

Table 5.4.6.1: Unauthorized Network Activities

Unauthorized Service	Reason
Chat/Instant Messaging	Security Vulnerability
ICQ - "I Seek You" - Internet chat paging program	Security Vulnerability

Unauthorized Service	Reason
IRC - Internet Relay Chat	Security Vulnerability
mIRC - Windows online chat program	Security Vulnerability
Net Meeting	Security Vulnerability
Realvideo	Excessive Bandwidth Usage
Quick Time	Excessive Bandwidth Usage
Peer-to-Peer (P2P) File Sharing[1]	Security Vulnerability and Excessive Bandwidth Usage

CBP-owned standalone computers may be used to connect to the Internet if the computers do not contain sensitive information and will not, at any time, be connected to a CBP network. In such cases, they are exempt from the Internet inter-connectivity policy. Other than standalone computers, the following rules apply for any connectivity of a CBP-owned system or network to the Internet or an Extranet:

1. Any connection of a CBP-owned system or network to the Internet or any approved Extranet must occur through an Office of Information and Technology (OIT)-provided secure gateway or firewall.

2. Connection of any CBP-owned classified system to the Internet or Extranet is strictly forbidden.

3. Any CBP-owned Intranet must be isolated and safeguarded from connectivity to the Internet or any Extranet.

4. Any CBP-owned server that stores non-public information for which an Internet or Extranet connection is approved must perform user identification and authentication for each user before allowing access. Identification and authentication will be performed in a secure manner not subject to disclosure or capturing. All passwords must be encrypted across the Internet or any Extranet.

[8]This is unauthorized for workstations. Network file sharing may be approved if it is justified and documented.

Securing Web Clients

Web technology is the part of network communications that allows parties to communicate using Hyper-Text Transfer Protocol (HTTP) or some variant of HTTP. Many of the security requirements of network communications apply directly to the use of Web technology, because Web technology is essentially an enhanced form of network communications.

The Web client and associated workstation must be appropriately configured to provide adequate security. At a minimum, the following requirements must be met:

1. All certificates must be protected with passwords that adhere to guidelines provided by the CISO. (A certificate is an association between an identity and a public key). Certificates are used as a way to verify the authenticity of an organization or individual.

2. Only certification authorities approved by the CISO may issue certificates that are installed on information systems that process sensitive or classified information. (A certification authority is an organization that issues public-key certificates.)

Securing Servers

Various Web technologies provide a convenient means for sharing information. Such technologies are examples of push/pull technology, which allow one entity to push information into a location and another entity to pull it from that location. Documents that an organization wishes to share with other organizations could be placed on (pushed out to) an external web and then anyone able to access the server could download (pull off) the information. Documents that an organization wishes to share internally could be placed on an internal (within an organization's system) Web, allowing authorized individuals within the organization to access the server download (pull off) the information. All servers must follow the guideline set forth within the ISVM notice published by DHS-SOC.

Servers can be separated into two broad categories: public or general access servers and restricted access servers. Descriptions of both types of servers are provided below:

Public or General Access Servers

Information placed on a public server is available to anyone authorized to access the Internet, Intranet, or a LAN on which the server resides. General user accounts are not permitted on public or general access servers.

Restricted Access Servers

Data placed on a restricted access server will only be accessed by authorized and authenticated users. In addition to the requirements stated earlier in this section, restricted access servers must also implement the following security requirements:

1. At a minimum, the underlying operating system must comply with the DHS security requirements for confidentiality, integrity, availability, and non-repudiation.

2. Strong authentication is required for all users accessing restricted servers; and all such accesses will be audited.

3. Web servers shall support secure Web technology. Unapproved web services on any device supporting such services shall be disabled in accordance with approved, standard CBP security configuration.

4. Web servers may not be enabled on routers, switches, printers, or workstations that are not authorized web servers configured to CBP standards. Any such operational web servers identified shall be disabled.

Mobile Code

Mobile code is Web-based code downloaded onto a user's client and run by the user's browser. Examples of such Web-based mobile code include Java, JavaScript, and ActiveX. A large set of mobile code normally involves an explicit decision to execute, either by the user or by an application. Examples of mobile code directly executed by the user include Perl, Tool Command Language/Tool Kit (TCL/TK), Restructured Extended Executor (REXX), Python, Visual Basic (VB), Java, and platform-specific executable(s), such as those with the filename suffix "com" or "exe."

Indirect execution of mobile code presents a significant security risk to systems connected to the Internet or external systems. Users may not even be aware that a separate executable has been downloaded on their machine. Examples of mobile code indirectly executed by an application include Microsoft (MS) Office macros, ActiveX, PostScript, and FileMaker. Hostile mobile code or executable content can introduce viruses or other malicious code to modify programs, allow unauthorized access, corrupt data, or deny service. Hostile mobile code or executable content is completely different from the more traditional malicious codes, such as viruses and worms. Moreover, they are probably not as detectable by standard antiviral software. Therefore, to reduce the risk of introducing hostile mobile code to the environment, CBP must implement security controls and policy for this technology.

Per DHS policy: "All mobile code (e.g., ActiveX, JavaScript) shall be reviewed and approved by an appropriate senior official before it is allowed to execute on DHS IT systems. Note: When the technology becomes available, the policy will be "Ensure that all approved mobile code (e.g., ActiveX, JavaScript) is digitally signed by the AO and that only signed code is allowed to execute on DHS IT systems."

The CISO has approved a mobile code policy that enables web-based access to external government (e.g. federal, state, and local law enforcement) systems that use mobile code when it enhances the user's ability to perform his/her job. This can be accomplished by adding the agency owning the web application to the user's list of trusted sites. However, these systems must undergo a review of their security controls. This could be accomplished via a review and/or testing by the LAN Engineering Team. In addition, an ISA must be in place with the external government agency owning the web-based application, which documents the security controls.

The table below categorizes types of mobile code based upon decreasing associated risk, with Category 1 representing the highest risk.

Table 5.4.6.4: Mobile Code Risk Categories

Mobile Code Category	Risk Level	Description	CBP Authorization Level
Category 1	Most dangerous	Includes ActiveX and script languages interpreted at the operating system command level, as well as newly emerging code not yet categorized.	Not allowed unless authorized by CBP management and additional security controls are in place. Signed code only, when technology is available.
Category 2	Moderately dangerous	Includes Java mobile code, PostScript, and various scripting languages running within the confines of a desktop application.	Authorized limited use, as permitted by workstation configuration security standards. Signed code only, when technology is available.
Category 3	Least dangerous	Includes Shockwave Flash content, Portable Document Format (PDF), VBScript, and European Computer Manufacture Association (ECMA) script-variant scripting languages interpreted within the confines of a browser.	Authorized limited use, as permitted by workstation configuration security standards. Signed code only, when technology is available.

1. Mobile code in new applications should be written and controlled so it can only be invoked as intended.

2. Internet Explorer must be configured to prevent the execution of unsigned Active-X code.

Use of mobile code in application development requires security review early in the design phase and potentially the submittal of a detailed request with justification to the Executive Director, Cyber Security Directorate. The CISO will review the associated risks with the designed implementation of this code and request approval from the AO, if appropriate.

Hypertext Transfer Protocol Secure (HTTPS)

Hypertext Transfer Protocol Secure (HTTPS) is the strongest privacy and integrity protection currently available for web connections. HTTPS provides integrity of the website and associated web servers with which one is communicating, which protects against man-in-the-middle attacks. Additionally, it provides bidirectional encryption of communications between a client and server, which protects against eavesdropping and tampering with or forging the contents of the communication. In practice, this provides a reasonable guarantee that one is communicating with precisely the website that one intended to communicate with (as opposed to an impostor), as well as ensuring that the contents of communications between the user and site cannot be read or forged by any third party. Websites and services available over HTTP must enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS going forward. HTTPS is a combination of HTTP and Transport Layer Security (TLS). TLS is a network protocol that establishes an encrypted connection to an authenticated peer over an untrusted network.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.6.5.a	CBP Current web site communication methods for web traffic should utilize the most secure method commercially available or as recommended by OMB guidance. This includes developing new and remediating legacy web sites to enforce HTTPS over TLS connections only (or HTTP HSTS redirects to HTTPS over TLS).	---
5.4.6.5.b	External Facing websites have HTTPS over TLS enabled up to the demarcation line (F5s) at which point traffic is decrypted and inspected by CBP SOC prior to re-encryption and forwarding to the end hosting servers.	---
5.4.6.5.c	All net new intranet sites internal to CBP utilize HTTPS over TLS wherever possible in order to reduce the risk of exploitation.	---

5.4.7 Email Security

All CBP personnel are reminded that there is no right of privacy in any CBP computer network system. CBP may access and disclose the contents of any electronic messages without consent of the owner/user when there is a legitimate business need, including but not limited to, the following circumstances:

1. In the course of an investigation or inquiry
2. For the protection and safety of CBP personnel
3. To prevent interference with the CBP mission
4. To locate information required for CBP business that is not more readily available by some other means

Email Bulletin Boards

Email Bulletin Boards are an approved method to provide information and notices to CBP personnel. Informational notices may include general notices, training seminars, facility information (e.g., power outages, system upgrades, training), office information (i.e., parties, death notices, leave share), medical services (i.e., flu shots, blood drives, health screenings), employee benefits (i.e., Thrift Saving Plan open season, Combined Federal Campaign), and Equal Employment Opportunity. The Help Desk, Technical Operations Division, will provide any assistance required in the operation or maintenance of a Bulletin Board.

The CBP email gateway Steward provides email monitoring for spam and virus activity at the gateway.

A relationship has been established with the SOC to enable communications. SOC personnel shall be trained to respond to incidents pertaining to email security and shall assist the email gateway Steward as necessary. CBP shall provide appropriate security for their email systems.

Email is the most commonly used application for exchanging data electronically. The email process can be divided into two main components: (1) mail servers, which deliver, forward, and store mail, and (2) clients, which interface with the user and allow them to read, compose, send, and store messages.

Instant Messaging (IM) and "I Seek You" (ICQ) tools provide similar capabilities to email but are inherently less secure; the technology to secure IM and ICQ tools is still being developed. IM and ICQ tools possess all of the risks associated with unsecured email, including the capability to install software or malware on a recipient's system without their knowledge. If IM and ICQ tools are to be used, they should not include or communicate with publicly available IM or ICQ tools provided by several Internet Service Providers. Any such tools employed need to be capable of blocking any format except pure text. This specifically includes blocking executable code, Web links, video or still images, and audio. The use of IM and ICQ is not currently authorized for use on sensitive systems and networks.

Second only to Web servers, mail servers are the host on a network that is most often targeted by intruders. Mail servers are targeted because they communicate, to some degree, with untrusted third parties. Additionally, email has been an effective method of passing malicious code

(viruses). As a result, mail servers, mail clients, and the network infrastructure that supports them must be protected. Email security issues include:

1. Flaws in the email application software have been used as the means of compromising the server and subsequently the associated network.
2. Denial of Service (DoS) attacks may be directed to the mail server.
3. Sensitive information on the mail server may be read by unauthorized individuals or changed in an unauthorized manner.
4. Unencrypted sensitive information transmitted between a mail server and email client could be intercepted.
5. Information within the email may be altered at some point between the sender and recipient.
6. Viruses and other types of malicious code may be distributed throughout an organization via email.
7. The sending of inappropriate, proprietary, or other sensitive information via email could expose an organization to legal action.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.7.a	CBP correctly secures, installs, and configures the underlying email operating system.	---
5.4.7.b	CBP correctly secures, installs, and configures mail server software.	---
5.4.7.c	CBP secures and filters email content.	---
5.4.7.d	CBP deploys appropriate network protection mechanisms, such as: – Firewalls – Routers – Switches – Intrusion Detection Systems (IDS)	---
5.4.7.e	CBP secures mail clients.	---
5.4.7.f	CBP conducts mail server administration in a secure manner. This includes: – Performing regular backups – Performing periodic security testing – Updating and patching software – Reviewing audit logs at least weekly	---
5.4.7.g	Auto forwarding or redirecting of DHS email to addresses outside of the .gov or .mil domain is prohibited and is not used. Users may manually forward individual messages after determining that the risks or consequences are low.	---
5.4.7.h	Classified information may not be posted in CBP unclassified environments or systems. Classified electronic messages are only transmitted through a secure data network approved for classified data.	---

Policy ID	CBP Policy Statements	Relevant Controls
5.4.7.i	Only personnel who have at least a completed Limited Background Investigation (BI) are granted access to the CBP email system. All email accounts are created, using at a minimum, the official last name as stated within the BI package.	---
5.4.7.j	Email addresses of CBP employees are not given to anyone without the express permission of the owner. Additionally, the requesting individual must substantiate that he/she has a valid need to obtain the information.	---
5.4.7.k	All material sent or received on the email system remains the property of CBP, not the property of the employee.	---
5.4.7.l	Everyone is responsible for preventing virus infections. Do not open attachments originating from unknown non-CBP addresses. Call your System Administrator (SA) for assistance.	---
5.4.7.m	Electronic messages are not used to send (upload), receive (download), or disseminate any material that is considered to be of a sensitive nature, without the express approval of its data owner.	---
5.4.7.n	Exercise care when using email to send extremely large files to distribution lists. Such a practice could lead to flooding of the network or denied services. There is a 10 MB size limit for email messages.	---
5.4.7.o	Capstone Accounts, annotated in General Records Schedule 6.1, are designated as permanent records. Additional details are available in the CBP RIM SharePoint site including the CBP RIM Directive, Handbook, Capstone Email Policy, Essential Records Plan, and EIS RIM Requirements.	---
5.4.7.p	All email communications of non-Capstone accounts are designated as temporary records with a 10-year retention period.	---
5.4.7.q	Email lists may be established to distribute mail to specific CBP populations. The mailing list owner is responsible for maintaining the list. The appropriate CBP management approves all messages addressed to 100 or more recipients before distribution. Personnel who do not adhere to this are subject to disciplinary action. Mass email lists of 500 people or more are only authorized for use under the following conditions: • National or CBP security, • Facility emergencies (e.g., facility closures, building evacuation), or • Announcements from CBP executive management.	---
5.4.7.r	Users may establish personal email lists. For organizational level email lists, a request is submitted through the Help Desk outlining the names, email addresses to be included, and a point of contact from	---

Policy ID	CBP Policy Statements	Relevant Controls
	the requesting office to act as the administrator for the maintenance of the list.	
5.4.7.s	Report suspected violations of electronic messaging policy to the SOC and notify your supervisor/manager if it is a significant incident. (See DHS 4300A Attachment F, *Incident Response* for details on incident reporting procedures and definitions of incidents.)	---
5.4.7.t	Creating, copying, transmitting, or retransmission of chain letters is strictly prohibited.	---
5.4.7.u	Transmitting sexually explicit or sexually oriented materials is strictly prohibited.	---
5.4.7.v	Disseminating offensive or disruptive messages that address topics such as a person's age, sexual orientation, religious or political beliefs, national origin, or disability is strictly prohibited.	---
5.4.7.w	Running a business from email is strictly prohibited.	---
5.4.7.x	Setting up personal accounts on the Internet and forwarding the information to a CBP email system is prohibited.	---
5.4.7.y	Using a CBP email address as a personal email address to receive advertisements is prohibited.	---
5.4.7.z	Sending documents in violation of copyright laws is strictly prohibited.	---
5.4.7.aa	Unauthorized viewing of electronic messages is strictly prohibited.	---
5.4.7.bb	Constructing electronic communication so it appears to be from someone else is strictly prohibited.	---
5.4.7.cc	Obtaining access to the files or messages of others with no substantial CBP business purpose is strictly prohibited.	---
5.4.7.dd	Attempting to breach security measures on any electronic messaging system is strictly prohibited.	---
5.4.7.ee	Attempting to intercept any electronic messaging transmissions without proper authorization is strictly prohibited.	---
5.4.7.ff	Forwarding email to home email accounts is prohibited.	---
5.4.7.gg	Common email naming conventions are implemented with distinguishing identifiers for non-CBP government employee email accounts that utilizes the following email display name suffixes and domains in the email system: • Contractor email accounts are identified by the "(CTR)" suffix in the email display name and the use of "@associates.cbp.dhs.gov" for the email domain. • Military officer email accounts are identified by the "(MIL)" suffix in the email display name and the use of"@military.cbp.dhs.gov" for the email domain.	---

Policy ID	CBP Policy Statements	Relevant Controls
	• Other U.S. Government Agency personnel email accounts are identified by the "(OGA)" suffix in the email display name and the use of "@OtherGovAgency.cbp.dhs.gov" for the email domain. • FSN/LES who are provided email access are identified by the (FSN) suffix in the email display name and the use of "@ForeignNational.cbp.dhs.gov" i.e., john.doe@ForeignNational.cbp.dhs.gov, DOE, JOHN (FSN).	
5.4.7.hh	All DHS email systems are required to use the common naming convention with distinguishing identifiers for military officers, contractors, foreign nationals, and U.S. Government personnel from other Departments and agencies.	---
5.4.7.ii	When sending email containing any unencrypted sensitive information, particularly sensitive PII, users should use caution. When sending such information outside the dhs.gov domain, users ensure that the information is encrypted. (See DHS Privacy Policy)	---
5.4.7.jj	Only Government email accounts are used to perform Government business.	---

Electronic Messaging and Email security responsibilities are provided below:

Electronic Messaging and Email Responsibilities
CBP CISO • Establishes policy to secure CBP email systems. • Advise on methods for securing CBP email systems. • Enforce CBP email security policies. **Security Control Assessors** • Conduct assessments to determine that adequate security controls are in place for email systems. **AO** • Ensure that adequate email security controls are in place prior to security authorization of the system. **System/Network Administrators** • Ensure email security controls are in place and functioning as intended. • Ensure email security controls provide the security features outlined in this document. • Correctly securing, installing, and configuring the underlying operating system. • Correctly securing, installing, and configuring mail server software. • Securing and filtering email content. • Updating and patching software must follow the guideline set forth in the Vulnerability

Electronic Messaging and Email Responsibilities

Management section of 1400-05D.
• Test and apply patches in a timely manner.
• Remove or disable unneeded services and applications on email servers.
• Configure user authentication for email systems.
• Review and analyze audit log at least weekly.
• Performing periodic security testing.
• Perform regular backups as required by the security plan.
• Protect email systems against malicious code.
• Deploy the following network protection mechanisms:
  o Firewalls
  o Routers
  o Switches
  o Intrusion detection systems
ISSOs
• Schedule semiannual/quarterly appointments with the SOC or Independent Verification and Validation (IV&V) team to scan the email system with a vulnerability assessment tool.
• Ensure that email system security controls are in place and functioning as intended.
• Ensure that email system security controls provide the security features outlined in this document and the security plan.
• Ensure a tested IT Contingency Plan is in place.

Securing a mail server is a two-step process. The first step is to secure the underlying operating system. Many security issues can be avoided if the operating systems are configured appropriately. The second step is to configure the email application. Administrators must configure their servers to apply the organization's security policy. Securing a mail server includes the following steps:

- Apply patches as they become available after first testing them in a lab environment
- Remove or disable unneeded services and applications
- Configure user authentication
- Scan the operating system with a vulnerability assessment tool

CBP must consider encryption technologies to protect their email systems. Most standard mail protocols default to unencrypted user authentication and send email data in the clear. Sending data in the clear allows a hacker to compromise a user's account and/or intercept emails.

When a Public Key Infrastructure (PKI) system is properly integrated into the client email facility, it is possible to "hash" a message to determine that it has not been altered or otherwise tampered with. It is also possible to encrypt sensitive data in an email using the employee's digital certificate encryption key and digitally sign an email using the digital certificate's signing key. This establishes integrity, confidentiality, and non-repudiation with regard to sensitive information.

The infrastructure that supports the network plays a vital role in the security of the email system. The network infrastructure is the first line of defense between the Internet and a mail server.

However, network design alone cannot protect a mail server. The following steps need to be accomplished on a regular recurring basis:

- Review and analyze log files
- Back up data daily (or in accordance with the security plan)
- Protect against malicious code (e.g., viruses, worms, Trojan horses)
- Have a recovery plan in the event of a disaster
- Test and apply patches in a timely manner
- Scan the system for vulnerabilities with a vulnerability-scanning tool

NIST SP 800-45, *Guidelines on Electronic Mail Security*, and NIST SP 800-49, *Federal S/MIME V3 Client Profile*, have valuable information detailing how to secure email. NIST SP 800-45 gives detailed technical guidance for Microsoft Exchange, Linux, and UNIX mail services and contains general guidance on how to secure mail servers.

5.4.8 Personal Email Accounts

As discussing sensitive information on a cell phone in a crowd can expose the information to untrusted ears, sending sensitive email to a personal account can expose that information to a large number of unauthorized individuals.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.8.a	The use of Internet webmail (Gmail, Yahoo, AOL) or other personal email accounts is not authorized over DHS furnished equipment or network connections except as provided in Section 1.11.1 of this policy handbook.	---
5.4.8.b	I do not provide personal or official DHS information solicited by e-mail.	---

Personal email responsibilities are provided below:

Electronic Messaging and Personal Email Responsibilities
CISO • Establishes policy concerning the transmittal of sensitive CBP information. • Evaluates the risks associated with the transmittal of sensitive information. • Evaluate the risks and recommend solutions to counter the risk of transmitting sensitive CBP information. **System Owners and Managers/Supervisors** • Enforce CBP policy prohibiting the transmittal of sensitive CBP information to personal email accounts. **System Administrators** • Ensure technical controls are in place and properly functioning to prohibit and/or deter the transmission of sensitive CBP information to personal email accounts. **ISSOs** • Ensure technical controls are in place and properly functioning to prohibit and/or deter the transmission of sensitive CBP information to personal email accounts.

Electronic Messaging and Personal Email Responsibilities
• Monitor compliance. **Users** • Comply with CBP policy prohibiting the transmission of sensitive CBP information to personal email accounts.

Sending email to a personal account has the following vulnerabilities:

1. Because personally owned computers are not authorized for use in CBP, they are not likely to have the appropriate encryption software installed, resulting in information sent in "clear text."
2. The route the email travels cannot be predicted.
3. Untrusted persons at Internet Service Provider (ISP) sites may read the sensitive information.
4. Because the email travels over unprotected communication links, it can be "sniffed" in transit and read by an unauthorized user.
5. Web browsers are often used to access private email accounts. Such access is inherently not secure.
6. Many worms and viruses, Malware (which could exist on the employee's personal computer) propagate themselves by mailing copies of existing emails or other text on a victim's computer to unknown individuals.
7. Instant Messaging (and Instant Chat Query (ICQ)) channels are a frequent source of viruses and mechanisms for attack of personal computers.
8. So-called "spy ware" programs transmit information from personal computers to sites unknown to the computer's owner. Many programs (both freeware and commercial) install these programs to harvest marketing information and other information from a user's computer.

Any unauthorized person who acquires sensitive information in this manner could post it on the Internet, deliver it to a news bureau, or forward it to individuals who could use the information to compromise national security.

5.4.9 Group Mailing

Group Mailing List (GML) is also known as distribution groups. These groups are used across CBP to disseminate information to large groups of employees in an efficient manner. If used improperly, GMLs can negatively impact CBPs email system and disrupt normal business activities. The following policy statements below will help to minimize potential impacts.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.9.a	GMLs are to be used only to disseminate CBP related information to groups of CBP staff. GMLs are restricted from containing external personal email addresses.	---
5.4.9.b	Two types of GMLs exist. • Small GMLs – Lists that contain fewer than 250 members must be	---

Policy ID	CBP Policy Statements	Relevant Controls
	approved by the Email Service Owner. • Large GMLs – Lists that contain 250 or more members must be approved by the OIT AC or the OIT DAC.	
5.4.9.d	GMLs are not created without one or more designated owners, an associated CBP office, and one or more authorized senders.	---
5.4.9.e	Upon GML creation and modification, designated owners are responsible for identifying an associated CBP office to which the GML belongs and one or more authorized senders. Designated owners are also responsible for maintaining the members of the GML. Authorized senders are individuals approved to send emails to the GML.	---
5.4.9.f	Before an email is sent, the GML(s) are inserted into the blind carbon copy (Bcc) field.	---
5.4.9.g	CBPs email Service Owner is accountable for oversight of the policy and routinely monitors the GMLs to ensure the designated owner(s), authorized sender(s), and a CBP office are assigned.	---
5.4.9.h	CBPs TSD is responsible for implementing the designated owner(s), CBP office and authorized sender(s) when creating a GML.	---
5.4.9.i	Exceptions to this policy are at the discretion of the OIT AC and based on mission critical needs.	---
5.4.9.j	Non-compliant GMLs are deactivated and removed from the Global Address List (GAL) promptly after their discovery.	---

5.4.10 Testing and Vulnerability Management

The DHS and CBP SOCs take a proactive approach to vulnerability management including detecting vulnerabilities through testing, reporting through ISVM messages, and conducting Vulnerability Assessments (VA).

Vulnerability management is a combination of detection, assessment, and mitigation of weaknesses within a system. Vulnerabilities may be identified from a number of sources, including reviews of previous risk assessments, audit reports, vulnerability lists, security advisories, and system security testing such as automated vulnerability scanning or security control assessments.

A core element of vulnerability management includes continuous monitoring and mitigating the discovered vulnerabilities, based on a risk management strategy. This strategy accounts for vulnerability severity, threats, and assets at risk. Risk calculation allows CBP to prioritize their remediation actions, in accordance with their specific situation and risk management strategy. Remediation actions are captured in CBPs patch management policy.

The DHS ISVM, managed through the DHS Security Operations Center (SOC), provides the CISO and security and operational personnel (e.g., CAs, ISSOs, LAN Administrators, System Administrators, Field Technology Officers) with bulletins, alerts, and technical advisories related to emerging vulnerabilities and threats. The ISVM is modeled on the Department of Defense's Information Assurance Vulnerability Assessment (IAVA) program but generally does not

prescribe the mitigation options nor centrally manage software patching. The following ISVM tools are available to support the CISO:

- CBP Top 20 Critical Vulnerabilities List
- DHS Vulnerability Assessment Team (VAT) – Red Team for Components without internal capabilities and for independent verification as necessary
- DHS Vulnerability Assessment Request Form (see Attachment O, *Vulnerability Management*)
- Negotiated pricing for VA tools (pending)

The DHS Vulnerability Management Program is described in 4300A Attachment O, *Vulnerability Management*. Testing and vulnerability assessments can be accomplished by a combination of scanning and manual techniques. Plans call for DHS to field an automated Security Authorization tool with a built-in vulnerability assessment capability. In addition, Plans of Action and Milestones (POA&Ms) will be prepared and used in conducting periodic vulnerability testing and assessments of information security controls and techniques.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.10.a	CBP conducts vulnerability assessments and/or testing to identify security vulnerabilities on information systems containing sensitive information annually or whenever significant changes are made to the information systems. This includes scanning for unauthorized wireless devices on the network. Evidence that annual assessments have been conducted is included with Security Assessment Reports (SARs) and with annual security control assessments.	---
5.4.10.b	The CISO and the SOC approves and manages all activities relating to requests for Vulnerability Assessment Team (VAT) assistance in support of incidents, internal and external assessments, and on-going System Engineering Life Cycle (SELC) support.	---
5.4.10.c	Anyone within CBP may request to be added to the ISVM distribution list. Those wishing to be added must provide a DHS email address and obtain management approval. ISVMs contain sensitive, "For Official Use Only," information and is not forwarded to non-DHS email accounts. • Although ISVM messages can be sent to anyone, only the CISO or their designated representatives acknowledges receipt of messages, report compliance with requirements or notify the granting of waivers.	SI-5
5.4.10.d	CBP reports compliance with the ISVM message within the specified timeframe. If unable to meet the designated compliance timeframe, CBP submits documentation of a waiver request via the DHS ESOC Online Portal (https://ecop.dhs.gov)	SI-5
5.4.10.e	CISO ensures coordination among the DHS ESOC, CBP SOC, and the ISVM Program when vulnerability assessment responsibilities	RA-3, AU-2

Policy ID	CBP Policy Statements	Relevant Controls
	encompass more than just CBP.	
5.4.10.f	The DHS and CBP SOCs are notified before any ISVM scans are run on a CBP Network.	RA-3, RA-5
5.4.10.g	System Owners report the security alert and advisory status of the information system to the CISO, AO, and DHS CISO upon request and on a periodic basis.	SI-5

Core elements of vulnerability management include continuous monitoring and mitigating the discovered vulnerabilities, based on a risk management strategy. This strategy accounts for vulnerability severity, threats, and assets at risk.

Testing and vulnerability assessment responsibilities are provided below:

Testing and Vulnerability Assessment Responsibilities
CISO and CBP SOC • Develop and follow POA&M procedures for implementing vulnerability assessments on sensitive systems. • Approve and manage all activities relating to requests for VAT assistance in support of incidents, internal and external assessments, and on-going SLC support. • Ensure coordination among the DHS ESOC, CBP SOC, and the ISVM Program when vulnerability assessments cross multiple Component responsibilities. **ISSOs and Information System Support Personnel** • Support SOC vulnerability assessments.

5.4.10.1 Vulnerability Scanning

Vulnerability scanning is the process of identifying known vulnerabilities of information systems operating on a network for the purpose of determining if and where a system can be compromised. Vulnerability scanning often employs software that contains a database of known flaws, tests systems for the occurrence of these flaws, and generates a report of the findings that the organization can use to tighten the network's security.

Vulnerability scanning typically refers to system audits on internal networks that are not connected to the Internet, as well as systems that are visible on the Internet, in order to assess the threat of rogue software and malicious or incompetent employees in an enterprise. Its purpose is to identify weaknesses in a system (or system security procedures, hardware design, internal controls, etc.) that could be exploited to gain unauthorized access to sensitive information or affect system availability or data integrity. Internal staff members who are part of the security staff performing this type of testing should have clearance levels commensurate with that of the system. These people shall intimately know the weaknesses of CBP IT systems and networks.

5.4.10.2 Expanded Vulnerability Scanning

The type of security testing performed by general-purpose vulnerability scanning tools may uncover weaknesses in the underlying components of systems that host CBP intranet or Internet web sites. A special class of scanning tools explores weaknesses in components of web systems for vulnerabilities related to the content and functionality of such systems. Examples of such vulnerabilities include the ability of unauthorized persons to examine or alter files, to establish cross-site scripting (which redirects users of a web site to another web site), or to directly access a database from which data is displayed on the website. A similar class of vulnerability tools exists for databases that have the capability of exploring inherent and design-induced weaknesses. Common vulnerabilities include default passwords that have not been removed, authentication bypass errors, and the ability to alter data without authentication.

Thorough vulnerability scanning expands upon the "canned" tools to include manual testing of potentially vulnerable systems and network components. For example, firewalls may provide barriers to standard discovery techniques. However, specialized scanning tools can utilize normally open ports (e.g., 80 for HTTP) and configurable timing parameters to discover internal systems in such a manner that neither a firewall nor a Network Intrusion Detection System (NIDS) can detect the scan. Such vulnerability assessments should also include both "war dialing" to find unauthorized dial-in modems, and "war driving" to detect unauthorized or misconfigured wireless network equipment.

5.4.10.3 Gap Analysis

One type of assessment is referred to as a "gap analysis". Such testing measures the deviations in installed systems and networks from the organization's stated policies and procedures. This type of analysis requires that the testers have access to internal information such as security policy and procedure documents and specific networks or systems that should be assessed. Internal staff or, preferably, third parties can perform gap analyses.

5.4.10.4 Penetration Testing

Penetration testing is a different process. Third-party personnel who have no knowledge of the security policies or the internal structure of the network typically perform penetration tests. Penetration testing assesses weaknesses of a computer facility or network to attack by amateur or professional "hackers." A thorough penetration test will include social engineering, dumpster diving, identification of networks through public sources (e.g., WhoIs and RwhoIs searches of the Regional Internet Registries) as well as manual techniques for finding weak points in an organization's perimeter. Once internal systems have been identified, a search of the NIST ICAT database can provide a laundry list of possible vulnerabilities in the hardware, operating systems, middleware, or applications discovered.

5.4.10.5 Scope of Vulnerability Assessments

All equipment attached to the CBP Network Infrastructure is subject to security vulnerability scanning. In today's changing environment, vulnerable and/or unprotected systems can easily be

overlooked. Systems that are not properly managed can become a potential threat to the health of the CBP infrastructure.

Proactive security scanning allows for a meaningful assessment of system security against known risks and provides a roadmap of effective countermeasures for improving security. Proactive scanning can also identify authorized and unauthorized devices on the internal network (e.g., unauthorized wireless access points, modems or high-speed Digital Subscriber Line (DSL) links installed by employees for their personal convenience without adequate security controls). Proactive scanning can lead to faster detection of vulnerabilities and can reduce damage to breached systems.

Reactive security scanning allows for threat quantification and assessment, accelerated damage control, and an assessment of systems against reasonable control measures during the repair/ rebuilding process.

Any system identified in conjunction with a security incident shall be subject to a comprehensive security scan. Random network scans shall not be advertised. Network and host scans shall be conducted by authorized DHS and/or CBP personnel using pre-designated scanning machines in order to be easily recognizable as benign activity in system log files. Because vulnerability scanning can be resource intensive, routine scanning is to be done during periods of low network activity when feasible.

5.4.11 Peer-to-Peer Technology

Peer-to-peer (P2P) technology is a phrase coined to apply to individual PCs acting as servers to other individual PCs. Made popular by the music file-swapping service Napster. Peer-to-peer technology allows users to share files with each other through a network of computers that use the same peer-to-peer client software. Each computer on the network has the ability to act as a both a server, by hosting files for others to download, and a client by searching other computers on the network for files the client wants to access.

This technology introduces a significant risk to Government data and exposes Government agencies to legal liability for copyright infringement. Use of this technology can also decrease productivity and use large amounts of bandwidth.

P2P applications circumvent most enterprise security systems. This provides malicious users easy access to a system, allowing them to install malware on participating systems, identify Internet Protocol (IP) addresses and usernames of internal machines, steal classified data, launch a denial-of-service attack (e.g., through bandwidth consumption, filling hard disks), or gain control of network resources.

P2P technology introduces a significant risk to Government data and exposes Government agencies to legal liability for copyright infringement. Use of this technology can also decrease productivity and use large amounts of bandwidth.

P2P computing or “file sharing” allows individual Internet users to connect to one another remotely with the intent of trading or sharing files. The use of external P2P software on CBP computers or on any computer or information system that might be connected to CBP networks

is prohibited. However, if the P2P connection is to a computer that is owned and managed by CBP, then the connection is permitted.

Although there are many appropriate uses of P2P computing, in its popular, more-common forms (e.g., Napster, Kazaa, and Grokster) studies have proven that a significant portion of shared files within P2P connections contain pornography and illegally obtained, copyrighted, music files. Further downloading P2P files can cause the CBP network to become vulnerable to a virus attack caused by downloading an infected file.

Instant Messaging is another common form of P2P networking. Use of commercial Instant Messaging applications such as AOL, MSN, and Yahoo is prohibited on CBP systems.

Many peer-to-peer programs do not allow users to control how much of their disk space is accessible, potentially allowing unauthorized persons access to files that the user has no intention of sharing.

In addition to security concerns, the use of peer-to-peer technology for its most commonly used functions (i.e., sharing music, images, and video) exposes both the individual and DHS to criminal prosecution for copyright violations.

For these reasons, peer-to-peer software is not authorized on DHS computers or on any computer or system that might be connected to the DHS network. Use of peer-to-peer software is considered an unauthorized use of Government resources and constitutes a reportable security incident and may result in sanctions against violators.

Policy ID	CBP Policy Statement	Relevant Controls
5.4.11.a	Software enabling publicly accessible peer-to-peer file sharing technology is not authorized on any DHS information system.	CM-7 CM-10

Peer-to-peer responsibilities are provided below:

Peer-to-Peer Technology Responsibilities
CISO • Establishes CBP policy regarding the unauthorized use of information technology and software. • Ensure that controls, including awareness training, are in place to minimize or prevent unauthorized use of unauthorized IT technology and software. **Supervisors** • Enforce unauthorized use policies including remedial training and other sanctions. • Promptly report unauthorized use of IT technology in accordance with 4300A Attachment F, *Incident Response.* **ISSOs/System/Network/LAN Administrators/FTOs** • Ensure that controls are in place including the use of monitoring and auditing to detect unauthorized use or installation of software. • Promptly report unauthorized use of IT technology in accordance with CBP Computer Security Incident reporting policy (DHS 4300A Attachment F, *Incident Response*). **Users** • Be aware of the prohibition against the use of unauthorized IT technology and software. • Adhere to the unauthorized use policies established in this section and in other references provided by CBP security officials. • Promptly report unauthorized use of IT technology in accordance with CBP Computer Security Incident reporting policy (DHS 4300A Attachment F, *Incident Response)*. • Be aware of and understand the ramifications of penalties involving infractions of the rules regarding inappropriate use of Government resources.

5.5 Scanning and Monitoring Policy

CBP-owned systems must be protected from all intrusions. Intrusions range from potentially damaging exploitation by adversaries to simple intrusion by inquisitive hackers. Occasionally, when the incident requires further action, monitoring of some type may be performed to both protect the critical system and to identify the perpetrator attempting to violate the security of the system. Any monitoring activities will be accomplished under the authority of the Office of Professional Responsibility. This section defines the policy on approved and prohibited actions involved with monitoring. It applies to all computer systems and networks within CBP. No matter which type of monitoring activity is being conducted, all personnel associated with the monitoring activity must be aware of the policies contained in this section.

IMPORTANT NOTICE

Unauthorized target monitoring is a violation of federal law and a subject's rights and could jeopardize any investigation or prosecution.

1. The SOC shall monitor the CBP network for security events using vulnerability scanners and Intrusion Detection System (IDS) technology.
2. A log-on warning banner is required on all networked and standalone CBP systems, regardless of the user. The warning banner must inform the user that he/she is subject to monitoring simply by using a government-owned system and as such there is no expectation of privacy. If the user does not consent to being monitored, he/she must be given the opportunity to exit before the log-on is completed.
3. Monitoring of a particular individual or group is prohibited without prior permission from the local IA Officer. Official procedures to initiate target monitoring are maintained and conducted by the Office of Professional Responsibility. Unless permission has been granted by IA to monitor a particular person, any monitoring must be broad-based, capturing all information on the monitored network, not just filtered information.
4. The requesting organization, usually IA, Chief Counsel, Labor and Employee Relations, or the Inspector General, will submit a written request for permission to conduct target monitoring. The SA must sign the request. It will then be sent through the local organization's Director and the local IA Officer, to the CISO. Approval must be obtained before target monitoring can begin. If there is an immediate need to begin monitoring because of acute mission requirements, the ISSO/SA shall honor the request and obtain the written permission after the fact. However, this is considered an exception to the policy; and the written request must be submitted as soon as possible. Please note, exceptions should only be granted when the requestor is one of the four organizations listed above, and the local IA Officer approves the action. All requests will include the following information:
    a. The date and time of the proposed monitoring
    b. Description of the planned activity including the identification of the network tool to be used
    c. A detailed explanation of the reason for the monitoring
    d. The anticipated results
    e. Signature of the SA
5. Target monitoring should always be conducted for the minimum amount of time. The System/Network/LAN Administrator, Field Technology Officer (FTO) or the ISSO must send a notification message to the CISO informing him/her of the monitoring activity. Any output provided by the monitoring shall be provided to the individual who requested the monitoring. The following information will be recorded by the SA and provided to the ISSO:

   a. When monitoring started and stopped
   b. A description of the activity with the identification of the monitoring tool used
   c. A detailed explanation of the reason for the monitoring
   d. Results of the monitoring
   e. Signature of the SA and ISSO
6. The SOC may conduct scheduled or unscheduled vulnerability assessments of any CBP asset at the direction of the CISO. The SOC is not required to obtain prior approval or notification for this type of vulnerability assessment.
7. The DHS-SOC shall be notified before any ISVM scans are run.

5.5.1 Authorized/Approved Monitoring

Actions to be taken when monitoring has been approved/authorized by the CISO:
Care must be taken NOT to destroy evidence, to implicate the innocent, or cause a subject to become aware of a planned monitoring activity. The ISSO (if available) and SA should make every effort to ensure that the following actions are performed in an orderly fashion.

1. Although backing up files may alter the associated properties (i.e., date last accessed), backup whatever files are deemed necessary in order to secure evidence.
2. Formally report the monitoring activity by sending an Incident Report in accordance with the SOC guidelines.
3. Initiate action to obtain permission from the CISO to implement monitoring procedures. The CISO is responsible for informing the AO.
4. Begin monitoring only after approval has been granted by the CISO.

Each person involved should be instructed to keep notes documenting the following items:

1. Names of people who have been briefed on the incident.
2. Names of people who may know about the incident without having been briefed.
3. A chronology of events from your personal knowledge.
4. Records of any correspondence generated on the incident.
5. Using the certification documentation and the security authorization package, review the functionality and structure of the system and document its location(s), hardware configuration, software applications, network connectivity, numbers of users, etc.
6. Keep a file of all correspondence relating to the incident.
7. Continually perform periodic backups as long as the activity continues.
8. Preserve the backups under lock and key as potential evidence.

5.5.1.1 Review System-Specific Features

The investigators will want full documentation on many aspects of the system being violated during the incident. The following questions are samples of those that may be used in the investigation. Not all of them apply to each incident, but all need to be reviewed to determine applicability. The ISSO and SA will make every effort to answer the following questions and document the information without arousing suspicion:

1. What event(s) triggered the suspicion of improprieties?
2. Does the system have a warning banner? Is the banner displayed before the first keystroke? Capture a copy of banner that was probably displayed.
3. Are any local operating procedures being violated?

4. Is there a copy of the Security Authorization Package available?
5. What is the function of the system?
6. What are the known system vulnerabilities?
7. Where is the hardware physically located?
8. What is the sensitivity level of the data processed on the system?
9. What organization/activity is supported by the system?
10. What internal and external connections are authorized to the system?
11. Are any of the connections supported by modems?
12. Is dial-in access authorized? If so, is it encrypted?
13. What are the baud rates of the modems used on the system?
14. What security software, if any, is used on the system?
15. What file transfer protocols are used on the system?
16. Are audit trails running normally; and have they been reviewed regularly?
17. Have vendor-supplied passwords been eliminated?
18. Are passwords machine-generated or selected by the user?
19. Have system passwords or the password file been stolen? Document the name of the password file, whether it was encrypted, and its location within the system.
20. How many failed log-on attempts were made in the last thirty days?
21. Who performs maintenance on the system; and do maintenance personnel have access to the system?

5.5.1.2 Review Actions of the Subject

The investigators will want information on the suspect. The ISSO and SA will make every effort to answer the following sample questions. Not all of the questions apply to every investigation. Review each question to determine its applicability. Document information on the following items without arousing suspicion:

1. Is the incident a repetitive act?
2. Is there a repetitive pattern to the time of the activity?
3. Is the subject an outsider? Is it possible to identify the person's nationality and affiliation?
4. If an insider, is the subject civil service, government contractor, etc.?
5. What is the subject's level of competency?
6. What is the subject's education level?
7. What is the subject's experience level?
8. What are the subject's responsibilities?
9. Does the subject have root-access privileges to the system?
10. Is there a current access control document signed by the subject?

11. What is the motive of the subject: amusement, competition, cover-up, financial or personal gain, protest, revenge, superiority, academic challenge, free flow of information, or other?
12. What computer protection schemes are used by the subject: automated batch files, encrypted files, Random Access Memory (RAM) disks, modified operating systems, trap doors in operating systems, archived or zipped files, bulk erasure, hidden files or directories, text files renamed as ".COM" or ".EXE" files, split files, files stashed on other computers, files stored in file slack areas of existing files, or any others?
13. What actions were taken by the subject to avoid identification: looping, stolen accounts, false accounts, deactivating audit trails, social engineering, manipulated programs, operating systems, or systems functions?
14. Did the subject download any of his/her own software to assist in his/her activities?

5.5.2 Sniffer Devices

A sniffer is a software program or hardware device, also known as a network or protocol analyzer, that intercepts routed data and can be used to examine each packet in search of specified information. Sniffers can be used for legitimate network management functions such as monitoring traffic for intrusion events and analyzing network problems. They can also be used to steal information from a network such as passwords transmitted in clear text. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere.

Any employee wishing to use sniffers must receive approval from the CISO or the AO. Currently, the CISO has limited the usage of sniffers within the CBP enterprise to the SO and the CBP Network Engineering Branch. Please consult the Enterprise Architecture (EA) team to obtain a list of CBP approved sniffers.

5.6 Cryptography

Cryptography provides a means for two or more parties to communicate securely. Cryptography is a branch of mathematics, which deals with the transformation of ordinary text (plain text) into coded form (ciphertext) by encryption and the transformation of cipher text into plaintext by decryption. Cryptography relies on two basic components: an algorithm (e.g., Advanced Encryption Standard (AES) and a key). The algorithm is the mathematical function used for encryption or decryption, and the key is the parameter used in the transformation.
There are two basic types of cryptography: secret key systems (also called symmetric systems) and public key systems (also called asymmetric systems).
In secret key systems, the same key is used for both encryption and decryption; that is, all parties participating in the communication share a single key that must be securely distributed and protected. In public key systems, each user is assigned his own pair of uniquely related keys: a private key known only to the key pair's owner, and a public key that can be made publicly available. Unlike secret key systems, the only keys that need to be shared are the public keys. The two keys are mathematically related, but the private key cannot be determined from the public key and the public key cannot be determined from the private key.

Encryption using a public key system works as follows:

1. The originator encrypts the communication for each intended recipient using each recipient's public key. A unique cyphertext is created for each intended recipient; the encryption is done by the PKI system and is transparent to the user.)
2. The encrypted message is sent to each recipient.
3. Each intended recipient uses his unique private key to decrypt the communication. This is done by the system and is transparent to the user.

Refer to NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government,* for more in-depth information on cryptography.

Digital signatures are implemented through a public key system. A digital signature is an electronic analogue of a written signature. Like a written signature, it can be used to (digitally) sign messages but has added advantages. Advantages include:

- Proving that the originator signed the message
- Determining whether or not the message was altered after it was signed
- Remotely authenticating a user's identity for access control
- Signatures may be generated for stored data and applications so that the integrity of the data and applications may be verified at any later time.

A digital signature is an electronic analogue of a written signature in that the digital signature can be used in proving to the recipient or a third party that the originator did in fact sign the message. Digital signatures may also be generated for stored data and programs so that the integrity of the data and programs may be verified at any later time. Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key that corresponds to, but is not the same as, the private key. The security of a digital signature system is dependent on maintaining the secrecy of users' private keys.

5.6.1 Encryption

Encryption is the process of changing plaintext into ciphertext for the purpose of security or privacy. It is a reliable and achievable way to help ensure confidentiality for sensitive data by converting plain text information into an unreadable form using approved algorithms. CBP employs encryption technologies to implement security requirements of certain data and in use of various devices, for example: passwords, symmetric and asymmetric keys, certain activities performed by system administrators and maintenance personnel, data packets transmitted on a wireless network, and data stored on laptop devices.

System specific encryption is addressed within the Security Authorization documentation using CBP-approved encryption methodologies.

Policy ID	CBP Policy Statements	Relevant Controls
5.6.1.a	Identify all IT systems transmitting sensitive information and determine if the system requires protection via encryption based on a risk assessment. If encryption is required, the following methods are used for encrypting sensitive information: • Products using FIPS 197 Advanced Encryption Standard (AES) algorithms with at least 256-bit encryption that have been	IA-7 SC-13

Policy ID	CBP Policy Statements	Relevant Controls
	validated under FIPS 140-2. A waiver is required for systems where AES cannot currently be used. • National Security Agency (NSA) Type 2 or Type 1 encryption. (Note: The use of triple Data Encryption Standard (3DES) and FIPS 140-1 is no longer permitted.)	
5.6.1.b	All CBP Major Applications (MAs) or General Support Systems (GSSs) with sensitive applications under their authority develops and maintains encryption plans for those information systems.	IA-7 SC-13
5.6.1.c	CBP uses only cryptographic modules that are FIPS 197 (AES-256) compliant and have received FIPS 140-2 validation at the level appropriate to their intended use.	IA-7, SC-13
5.6.1.d	Application-level encryption or an encrypted virtual private network link are used for any sensitive data that is transmitted over the Internet or other public network.	IA-7 SC-13

CBP Encryption responsibilities are provided below:

CBP Encryption Responsibilities
AO • Ensure sensitive or classified encryption applications under their authority have developed encryption plans for systems prior to security authorization. • Ensure personnel implementing encryption requirements are technically qualified and adequately trained in encryption technologies and specific methodologies employed. **CBP CISO** • Ensure CBP encryption policy is implemented and enforced. • Advise project managers on the implementation of CBP encryption standards. **ISSOs** • Ensure CBP encryption methodology is properly implemented and configured on all required CBP IT systems. • Assist system owners in identifying sensitive CBP data that requires encryption.

Encryption is a reliable and achievable way to help ensure confidentiality for sensitive data. It involves converting plain text information into an unreadable form using approved algorithms. DHS employs encryption technologies to implement requirements. These requirements include encryption of passwords, symmetric and asymmetric keys, certain activities performed by system administrators and maintenance personnel, data packets transmitted on a wireless network, and data stored on laptop devices.

CBP shall ensure that encryption is addressed in the Security Authorization documentation using DHS-approved encryption methodologies.

5.6.2 Public Key Infrastructure

In the past, communications involving sensitive data could not be conducted securely through purely electronic means. With the advent of Public Key Infrastructure (PKI), securing the exchange of sensitive messages while providing limited access to public information networks became available. DHS implemented a PKI program that consists of products and services to provide standard public key certificates for use throughout the organization. DHS mandated the use of PKI throughout its Components. The E-Gov Act also requires such use of PKI to improve network authentication.

A Public Key Infrastructure (PKI) is an architected set of systems and services that provide a foundation for enabling the use of public key cryptography. This is necessary in order to implement strong security services and to allow the use of digital signatures.
The principal Components of a PKI are the public key certificates, registration authorities (RA), certification authorities (CA), directory, certificate revocation lists (CRL), and a governing certificate policy (CP).

PKI provides the means to bind public keys to their owners' private keys and helps in the distribution of reliable credentials in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates, which contain information such as the owner's name and the associated public key, are issued by a reliable Certification Authority (CA). Reliable identification of individuals is an inherently governmental activity. In order to establish and maintain the trust required to support DHS missions, the root certificate must be controlled by the DHS. DHS implemented a PKI program that consists of products and services to provide standard public key certificates for use throughout the organization. DHS mandated the use of PKI throughout its Components. The E-Gov Act also requires such use of PKI to improve network authentication. The DHS PKI shall be governed by a DHS X.509 Certificate Policy (DHS CP).
Specific requirements for PKIs which must be met are detailed in DHS Sensitive Systems Policy Directive 4300A.
PKI provides the means for an organization to meet four critical security objectives:

1. Authentication
2. Non-Repudiation
3. Data Integrity
4. Confidentiality

PKI usually consists of:

1. A Certificate Authority that issues and verifies a digital certificate. A certificate includes the public key or information about the public key.
2. A Registration Authority (RA) that acts as the verifier for the Certificate Authority before a digital certificate is issued to a requestor.
3. One or more directories where the public key portion of the certificate resides.
4. A certificate management system.

PKI systems enable users of an unsecured network to securely and privately exchange information using private and public key pairs. In public key cryptography, a public key and a

private key are created simultaneously using the same algorithm. Public keys are bound to their owners by public key certificates. These certificates, which contain information such as the owner's name and the associated public key, are issued by a reliable CA. The Certificate Authority gives the private key only to the requesting party and makes the public key available (as part of a digital certificate) in a directory that all parties can access. The authorized owner uses a private key to decrypt text that has been encrypted with the public key by someone else. PKI also provides a digital certificate that can be used to electronically 'sign' documents.
All CBP departments, employees, and contractors are considered 'Relying Parties' who:

1. Check each digital certificate for its validity or revocation prior to issuance.
2. Verify the receipt of the digital signature of a digitally signed message.
3. Verify the digital signature of the Certificate Authority who issued the certificate.

DHS Certification Practices Statements (CPS) and the corresponding DHS Certificate Policy mandate guidelines on the intended use of PKI certificates. All CBP employees, and contractors are required to follow the enrollment and registration procedures set forth in these DHS PKI policy documents.

Employees and contractors obtain sponsorship for certificates through their respective managers. PKI enrollment procedures for CBP require completion of the following forms before an individual is issued a digital certificate:

1. Pre-Enrollment Subscriber Form
2. Human Subscriber Agreement Form
3. Local Registration Authority (LRA) Nomination Form
4. Sponsor Form
5. In person identity proofing (with two forms of identification)
6. On-line Certificate Request application and key pair generation

The CISO nominates trusted individuals for trusted roles before subscriber registration can begin. LRAs and Trusted Agents (TAs) obtain smartcards and smartcard readers to implement this technology. Smartcards are able to store and process information. Users are issued a smartcard that stores data such as the PKI private key, personal ID with photo, building access card, and parking permit.

Policy ID	CBP Policy Statements	Relevant Controls
5.6.2.a	DHS implements two distinct PKIs: **DHS Federal PKI (FPKI):** DHS shall implement a DHS Public Key Infrastructure (PKI) that is part of the FPKI to facilitate the use of PKI within DHS, and to facilitate the interoperable use of PKI between DHS and its external mission and business partners, such as other Federal agencies; state, local and tribal governments; public and private sector entities; and U.S. citizens.	SC-17

Policy ID	CBP Policy Statements	Relevant Controls
	DHS Internal Use NPE PKI: At the DHS Enterprise-level, a single DHS Enterprise Internal Use Non-Person Entity (NPE) PKI may be implemented to issue certificates to DHS NPEs to support NPE-to-NPE authentication across DHS networks, where the certificates have no external relying parties. At the DHS Component-level, CBP may implement one or more DHS Internal Use Non-Person Entity (NPE) PKIs consisting of individual DHS Component PKIs for use solely by that Component to issue certificates to that Component's NPEs to support NPE-to-NPE authentication on that Component's networks, where the certificates have no external relying parties.	
5.6.2.b	The DHS CISO is the DHS PKI Policy Authority (PKIPA) to provide PKI policy oversight for all DHS PKIs. **DHS FPKI:** A detailed description of DHS PKIPA roles and responsibilities are provided in the Registration Practice Statement for the DHS Principal Certification Authority. **DHS Internal Use NPE PKI:** A detailed description of DHS PKIPA roles and responsibilities are provided in the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines.	SC-17
5.6.2.c	The DHS CISO represents DHS on the Federal PKI Policy Authority (FPKIPA).	SC-17
5.6.2.d	The DHS PKIPA appoints a PKI Management Authority (PKIMA) to provide management and operational oversight for all DHS PKIs. **DHS FPKI:** A detailed description of DHS PKIMA roles and responsibilities are provided in the Registration Practice Statement for the DHS Principal Certification Authority. **DHS Internal Use NPE PKI:** A detailed description of DHS PKIMA roles and responsibilities are provided in the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines.	SC-17
5.6.2.e	**DHS FPKI:** CBP CISO is responsible for management oversight of the DHS PCA RA activities and personnel within CBP.	---
5.6.2.f	**DHS FPKI:** The DHS FPKI is governed by the U.S. Common Policy Framework certificate policy approved by the FPKIPA, and by the relevant portions of the Department of the Treasury Public Key Infrastructure	SC-17

Policy ID	CBP Policy Statements	Relevant Controls
	(PKI) X.509 Certificate Policy approved by the Department of the Treasury Policy Management Authority (PMA). **DHS Internal Use NPE PKI:** The DHS Internal Use NPE PKIs are governed by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines approved by the DHS PKIPA.	
5.6.2.g	**DHS FPKI:** DHS has a single DHS Principal CA (i.e., DHS CA4) that has the U.S. Common Policy Root CA as its trust anchor. The DHS Principal CA is operated for DHS by the Department of Treasury under the Federal Shared Service Provider (SSP) program.	SC-17
5.6.2.h	**DHS FPKI:** The DHS Principal CA is the only DHS CA subordinated to the Treasury Root CA. Additional DHS CAs subordinate to the DHS Principal CA are not permitted. **DHS Internal Use NPE PKI:** A single DHS Enterprise Internal Use Non-Person Entity (NPE) PKI may be implemented. CBP may implement one or more DHS Internal Use NPE PKIs. Each PKI is a hierarchical PKI with one or more levels. • For a single-level hierarchy, the PKI consists of a single self-signed Internal Use NPE CA. • For a two-level hierarchical, the PKI consists of a single self-signed Internal Use NPE Root CA at the top level, and one or more Internal Use NPE CAs that are each directly subordinated to the Internal Use NPE Root CA. • Additional Internal Use NPE CAs may be directly subordinated to an existing subordinate Internal Use NPE CA, thereby adding an additional level to the hierarchy. The requirements and process for implementing a DHS Enterprise Internal Use NPE Root and Subordinate CA and for implementing a CBP Internal Use NPE PKI Configuration and Operation Practices Guidelines.	SC-17
5.6.2.i	**DHS FPKI:** The DHS Principal CA has a trust path resolving to the U.S. Common Policy Root CA via the Treasury Root CA. Establishing direct trust relationships with any other CAs is not permitted. The U.S. Common Policy Root CA is cross certified with the Federal Bridge CA at the high, medium hardware, and medium assurance levels. **DHS Internal Use NPE PKI:**	SC-17

Policy ID	CBP Policy Statements	Relevant Controls
	If a DHS Internal Use NPE PKI consists of a single NPE CA, the CA is self-signed and function as its own trust anchor. If a DHS Internal Use NPE PKI is a multi-level hierarchical PKI, with a Root and subordinate CAs, the trust path from subordinate CAs resolve to the Root CA as the PKIs trust anchor. A request to implement trust relationships between CBP Internal Use Non-Person Entity (NPE) PKIs, or between the DHS Enterprise Internal Use Non-Person Entity (NPE) PKI and a CBP Internal Use Non-Person Entity (NPE) PKI are submitted to the DHS PKIMA for review and approved by the DHS PKIPA.	
5.6.2.j	**DHS FPKI:** The DHS Principal CA operates under an X.509 Certification Practice Statement (CPS). The CPS comply with the U.S. Common Policy Framework and the Treasury Certificate Policy. Since the Department of the Treasury, as the SSP for DHS, operates the DHS Principal CA, the Department of the Treasury PKI Policy Management Authority, approves the CPS for the DHS Principal CA. DHS operates two Registration Authorities for the DHS Principal CA (PC4). The DHS PCA Registration Authority (DHS PCA RA) is responsible for performing the life-cycle administration for non-PIV certificates, and the DHS PCA PIV Registration Authority (DHS PCI PIV RA) is responsible for performing the life-cycle administration of PIV certificates. The two DHS Registration Authorities for the DHS Principal CA operates under the Registration Practice Statement for the DHS Principal Certification Authority (RPS). The RPS is approved by the DHS PKIMA and the DHS PKIPA and approved for conformance to the U.S. Common Policy Framework and the Treasury Certificate Policy by the Department of the Treasury PKI Policy Management Authority. **DHS Internal Use NPE PKI:** DHS Internal Use NPE CAs operate under the DHS Internal Use NPE PKI Configuration and Operation Practices Guide (COPG) which are approved by the DHS PKIPA.	SC-17
5.6.2.k	**DHS FPKI:** The DHS PKIMA ensures that the DHS PCA Registration Authority (DHS PCA RA) operates in compliance with the RPS. The DHS PIV Card Issuer (PCI) Organization Identity Management Official (DHS OIMO) ensures that the DHS PCA PIV Registration Authority (DHS PCI PIV RA) operates in compliance with the RPS. **DHS Internal Use NPE PKI:**	SC-17

Policy ID	CBP Policy Statements	Relevant Controls
	The DHS PKIMA ensures that every DHS Internal Use NPE CA operates in compliance with the DHS Internal Use NPE PKI Configuration and Operation Practices Guide (COPG).	
5.6.2.l	**DHS FPKI:** The DHS Principal CA undergoes regular PKI compliance audits as required by the U.S. Common Policy Framework. The audit findings, report, and Plans of Action and Milestones (POA&Ms) that address deficiencies found are provided to the DHS PKIPA and DHS PKIMA. **DHS Internal Use NPE PKI:** Every DHS Internal Use NPE CA undergoes regular PKI compliance assessments as required by the DHS Internal Use NPE PKI COPG. The assessment findings, report, and Plans of Action and Milestones (POA&Ms) that address deficiencies found, are provided to the DHS PKIPA and DHS PKIMA.	SC-17
5.6.2.m	**DHS FPKI**: The DHS Principal CA archives records as required by the U.S. Common Policy Framework, the Treasury Certificate Policy, and the DHS Principal CA CPS. **DHS Internal Use NPE PKI:** Every DHS Internal Use NPE CA (Root and Subordinates) archives records as required by the DHS Internal Use NPE PKI COPG.	SC-17
5.6.2.n	**DHS FPKI:** All operational PKI facilities are established in accordance with U.S. Common Policy Framework physical security requirements based on the CA's assurance level and its intended use. Location/protection of the CA are determined by its level of assurance. Measures taken to ensure the continuity of PKI operations shall provide at least the same level of PKI Services availability as the individual and composite availability requirements of the systems and data protected by the certificates.	SC-17
5.6.2.o	**DHS FPKI:** The DHS Principal CA only issue certificates to internal DHS entities, e.g., Person Entities (PEs) such as employees, contractors, affiliates, roles, groups, and NPEs such as hardware devices, systems, and applications. External entities that require certificates to securely interact with DHS acquire the certificates from: (1) another Federal Agency's PKI or SSP PKI operating under the U.S. Common Policy Framework or (2) a non-Federal Agency PKI that is cross-certified with the FBCA at medium, medium Hardware, PIV-I, or high assurance level). **DHS Internal Use NPE PKI:**	SC-17

Policy ID	CBP Policy Statements	Relevant Controls
	DHS Enterprise Internal Use Non-Person Entity (NPE) CAs only issues authentication certificates to DHS Component NPEs (i.e., internal hardware devices and systems) when any of the following conditions apply: • There are no relying parties for the certificates external to the DHS Component • The certificates are only used for authentication • The certificates are explicitly authorized to be issued by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines (COPG) CBP Internal Use NPE Root CA may issue a CA certificate to subordinate CBP Internal Use NPE CA for CBPs Root CA. A CBP Internal Use NPE CA may issue a CA certificate to subordinate a CBP Internal Use NPE CA to itself.	
5.6.2.p	**DHS FPKI:** Only the DHS Principal CA issue certificates to DHS PEs, i.e., DHS employees, contractors, affiliates, roles and group entities. Types of PE certificates that may be issued include authentication, digital signature verification and encryption certificates, including certificates for DHS HSPD-12 Personal Identity Verification (PIV) Cards, code signing and content signing, as well as all other types of certificates allowed under the U.S. Common Policy Only the DHS Principal CA shall issue certificates to DHS NPEs, i.e., hardware devices, systems and applications, when the following conditions apply:• • There are external relying parties for the certificates • The certificates are used to protect sensitive DHS data or to authenticate to operational systems containing sensitive data, and • The certificates are not explicitly authorized to be issued by DHS Internal Use NPE CAs in the DHS X.509 Internal Use NPE Certificate Policy.	SC-17
5.6.2.q	**DHS FPKI:** The Treasury Root CA is used by Relying Parties in DHS as the trust anchor for the validation of certificates issued by the DHS Principal CA (DHS CA4). The U.S. Common Root CA is used by Relying Parties external to DHS as the trust anchor for the validation of certificates issued by the DHS	SC-17

Policy ID	CBP Policy Statements	Relevant Controls
	Principal CA (DHS CA4). The U.S. Common Root CA is also used by Relying Parties in DHS as the trust anchor for the validation of certificates issued by CAs external to DHS.	
5.6.2.r	The use by DHS of any non-DHS PKI provider for CA or PKI services is prohibited unless approved by the DHS CISO on a case-by-case basis.	SC-17
5.6.2.s	DHS FPKI: Only certificates that are issued by the DHS Principal CA under the U.S. Common Policy Framework at medium assurance or above are used to protect sensitive DHS data or to authenticate to operational systems containing sensitive data. Certificates issued by test, pilot, third party, self-signed or other CAs are not used to protect sensitive information, or to authenticate to DHS operational systems containing sensitive data. **DHS Internal Use NPE PKI:** Certificates issued by DHS Internal Use NPE CAs, are only used for authentication.	SC-17
5.6.2.t	**DHS FPKI:** For all external-facing DHS web services, compliance with OMB Memorandum 15-13 and 17-06 (use of HTTPS and HSTS) is mandatory. Federally issued certificates will not be practical for web services whose users may not always be expected to trust the issuing federal certificate authority. These web services will likely require the use of a certificate from a publicly trusted (commercial) certificate authority. These should be obtained after approval by the DHS CISO. DHS CA4-issued certificates may be practical for web services whose users can be consistently expected to trust the issuing DHS certificate authority or the federal CA trust anchor it chains to.	SC-17
5.6.2.u	Commercial applications or appliances used by DHS that require the use of PKI certificates obtain those certificates from the DHS Principal CA or a DHS Component Internal Use NPE CA, as appropriate. Commercial applications or appliances, that require the use of a proprietary CA implemented as an internal feature, are not acquired or used, unless prior concurrence by the DHS PKIMA and approval by the DHS PKIPA are obtained.	SC-17
5.6.2.v	Certificate trust stores contain root certificates, each of which is the trust anchor for a PKI. Certificates in trust stores are implicitly trusted by certificate validation software. Vendors' products come pre-	SC-17

Policy ID	CBP Policy Statements	Relevant Controls
	populated with many root certificates in their trust stores, including certificates for PKIs that DHS does not want to implicitly trust. CBP manages the content of installed product's trust stores, including: • Leveraging automated management, such as with Microsoft Group Policy Objects (GPOs) • Removing all certificates that have passed their expiration date • Removing all certificates that are no longer trusted • Removing all certificates that are no longer required	
5.6.2.w	Commercial products used by DHS and applications developed by DHS that enable the use of PKI at a minimum support the following cryptographic algorithms and associated key sizes: • SHA 1 • SHA 256 • RSA with 1024 Bit keys • RSA with 2048-bit keys • AES 128 • AES 256	SC-17

Implementation of public key infrastructure (PKI) technology, utilizing data encryption, ensures that cryptographic security goals are met. When used either separately or in conjunction with PKI, a virtual private network (VPN) greatly enhances secure data transmission, especially when encryption techniques are employed.

5.6.3 Public Key/Private Key

The recipient of public key certificates is referred to as a subscriber. A subscriber can be a human (e.g., an employee or contractor), an organization, an application, a code signer (e.g., digitally signs released software to enable users to authenticate its source, legitimacy, and integrity), or a device (e.g., a web server or VPN server). Registrars are trusted PKI officials who administer the process that results in a CA issuing or revoking public key certificates for each subscriber. As part of the PKI registration process, a public key/private key pair is generated in a hardware or software cryptographic module that is under the control of the subscriber. The private key remains under the sole possession of the subscriber. A CA enters the public key into an electronic public key certificate that also identifies the owner of the key, i.e. the subscriber. The trusted CA digitally signs the certificate thereby binding the public key to the subscriber and makes the signed certificate available for use by other subscribers.

A subscriber's public key certificate is used by other subscribers, referred to as relying parties, to obtain the subscriber's public key in a trusted manner. Once obtained, the public key is then used: (1) to encrypt data for that subscriber so that only that subscriber can decrypt it with their private key, or (2) to verify that digitally signed data was signed by that subscriber using their

private key, thereby authenticating the identity of the signing subscriber, and the integrity of the signed data.

A public key/private key pair validated in accordance with Federal Information Processing Standard (FIPS) 140-1 is generated in a hardware or software cryptographic module as part of the PKI registration process and is under the control of the subscriber. The private signing key remains under the sole possession of the subscriber; it is escrowed by the CA and may be securely recovered if it is lost or corrupted. This practice allows previously encrypted data to be decrypted by the subscriber.

Policy ID	CBP Policy Statements	Relevant Controls
5.6.3.a	**DHS FPKI:** A single public/private key pair is not used by a human subscriber for both encryption and digital signature.	SC-12
5.6.3.b	A single public/private key pair is not used by an NPE for both encryption and digital signature, whenever their separate use is supported by the protocols native to the NPE.	SC-12
5.6.3.c	An authorized human sponsor represents each role, group, code-signer, system, application and device subscriber when the subscriber applies for one or more certificates from a DHS CA.	SC-12
5.6.3.d	**DHS FPKI:** An authorized DHS employee sponsors DHS contractors or other affiliates who apply for one or more certificates from a DHS CA.	SC-12
5.6.3.e	A mechanism is provided for each DHS CA to enable PKI registrars to determine the eligibility of each proposed human, role, group, code signer, system, application, or device to receive one or more certificates.	SC-12
5.6.3.f	A mechanism is provided for each DHS CA to enable PKI registrars to determine and verify the identity of the authorized human sponsor for each DHS contractor, affiliate, role, group, code signer, system, application, or device.	SC-12
5.6.3.g	DHS FPKI: Human subscribers do not share their private keys and are responsible for their security and use. If a human subscriber discloses or shares his or her private key, the subscriber is accountable for all transactions signed with the subscriber's private key.	SC-12
5.6.3.h	**DHS FPKI:** Sponsors for non-human subscribers (systems, application and devices,) are responsible for the security of and use of the subscriber's private keys. Every sponsor reads, understands, and signs a "DHS PKI Device Sponsor Acknowledgement of Responsibilities" as a pre-condition for sponsoring non-human subscribers.	SC-12

Policy ID	CBP Policy Statements	Relevant Controls
5.6.3.i	Subscriber private keys are not used by more than one entity, with the following exceptions: • Authorized members of a Group Subscriber, may use the Group's private keys. • Multiple systems or devices in a high availability configuration may use a single Key pair providing the Subject Alternative Name (SAN) field within the SSL certificate identifies all of the devices with which the key is to be shared.	SC-12
5.6.3.j	**DHS FPKI:** Every human subscriber reads, understands, and signs a "DHS PKI Human Subscriber Acknowledgement of Responsibilities" as a pre-condition for receiving certificates from a DHS CA. Signed PKI Human Subscriber Agreements are maintained by the DHS PKI Registrar.	SC-12

Public key/private key responsibilities are provided below:

Public Key/Private Key Responsibilities
DHS CISO • Ensures that the DHS CP and CPSs enforce the use of separate public/private key pairs for encryption and digital signature by human subscribers, organization subscribers, application subscribers, code-signing subscribers, and also by device subscribers whenever supported by the protocols native to the type of device. • Ensures that the DHS CP and CPSs require that a human sponsor shall represent each organization, application, code-signing, and device subscriber when it applies for one or more certificates from a DHS CA. • Ensures that DHS CPSs require that a mechanism is provided for each DHS CA to enable PKI registrars to determine the eligibility of each proposed human, organization, application, code signer, or device subscriber to receive one or more certificates. • Ensures that controls are implemented to hold human subscribers accountable for the security of their private key and for all transactions signed with their private key. • Ensures that controls are implemented to hold the sponsor of an organization, application, code signing, or device subscriber responsible for the security of and use of the subscriber's private keys. • Ensures that controls are implemented to maintain individual accountability for each use of a shared organizational or code signing private key. • Ensures that a DHS PKI Subscriber Agreement for Human Users and a DHS PKI Subscriber Agreement for Sponsors are created and maintained, and that DHS CPSs require human subscribers and sponsors to read, understand, and sign them as a pre-condition for receiving certificates.

Public Key/Private Key Responsibilities
DHS PKI Operational Authority • Ensures that the DHS CPSs and operating procedures enforce the use of separate public/private key pairs for encryption and digital signature by human subscribers, organization subscribers, application subscribers, code-signing subscribers, and also by device subscribers whenever supported by the protocols native to the type of device. • Ensures that the DHS CPSs and operating procedures require that a human sponsor shall represent each organization, application, code-signing, and device subscriber when it applies for one or more certificates from a DHS CA. • Verifies that that a mechanism is provided for each DHS CA to enable PKI registrars to determine the eligibility of each proposed human, organization, application, code signer, or device subscriber to receive one or more certificates. • Verifies that a mechanism is provided for each DHS CA to enable PKI registrars to determine the authorized human sponsor for each organization, application, code signer, or device. • Verifies that controls are implemented to hold human subscribers accountable for the security of their private key and for all transactions signed with their private key. • Verifies that controls are implemented to hold the sponsor of an organization, application, code signing, or device subscriber responsible for the security of and use of the subscriber's private keys. • Verifies that controls are implemented to maintain individual accountability for each use of a shared organizational or code signing private key. • Ensures that DHS CPSs and Operating Procedures require human subscribers and sponsors to read, understand, and sign DHS PKI Subscriber Agreements as a pre-condition for receiving certificates. **DHS Office of Security** • Provides a mechanism, as required by the CPS, to enable PKI registrars to determine the eligibility of each proposed human subscriber to receive one or more certificates from the DHS CA. • Ensures that registrars under their purview require human subscribers and sponsors to read, understand, and sign DHS PKI Subscriber Agreements as a pre-condition for receiving certificates. **CISO** • Provide a mechanism, as required by the CPS, to enable PKI registrars to determine the eligibility of each proposed human subscriber to receive one or more certificates from the DHS CA. • Provide a mechanism, as required by the CPS, to enable PKI registrars to determine the authorized human sponsor for each organization, application, code signer, or device. • Implement controls to hold human subscribers accountable for the security of their private key and for all transactions signed with their private key.

Public Key/Private Key Responsibilities
• Implement controls to hold the sponsor of an organization, application, code signing, or device subscriber responsible for the security of and use of the subscriber's private keys. • Implement controls to maintain individual accountability for each use of a shared organizational or code signing private key. • Ensure that registrars under their purview require human subscribers and sponsors to read, understand, and sign DHS PKI Subscriber Agreements as a pre-condition for receiving certificates. **ISSOs** • Ensure human subscribers are aware of their responsibilities to protect their private keys. • Ensure sponsors are aware of their responsibilities to protect the private keys of the subscriber they sponsor. • Maintain auditable records to ensure individual accountability is maintained for each use of an organization or code-signing private key authorized for use by more than one person. **Human Subscribers** • Assume responsibility for the security of their private keys. • Abide by the DHS PKI Subscriber Agreement for Human Users that they signed and review it at least annually. **Sponsors** • Assume responsibility for the security of the private keys of the subscribers they sponsor. • Abide by the DHS PKI Subscriber Agreement for Sponsors that they signed and review it at least annually.

CBP employees and contractors should have reasonable assurance that, when initiating a secure transaction:

1. The information sender and recipient both will be identified uniquely so that both parties know not only where the information originated but also its destination.
2. The information was not altered deliberately or inadvertently.
3. The sender's identity is inextricably linked to the transmitted information.
4. The information will be protected from unauthorized use.

5.7 Malware Protection

There are a number of programs that are classified as malicious code, or "malware." These programs are referred to as viruses, logic bombs, worms, Trojan horses, and other names. This section covers types of malware.

Computer viruses pose an ever-increasing problem for applications, systems, and networks. All DHS organizations must implement appropriate file, protocol, and content filtering activities to protect their modification by computer viruses. Malicious code includes, but is not limited to, viruses, logic bombs, worms, Trojan horses, and similar software-induced problems.

Policy ID	CBP Policy Statements	Relevant Controls
5.7.a	The CISO establishes and enforces CBP malware protection control policies.	SI-3 SC-5
5.7.b	CBP implements a defense-in-depth strategy that: • Installs anti-malware software on desktops and servers • Configures anti-malware software on desktops and servers to check all files, Internet downloads, and email. • Installs updates to anti-malware software and signature files minimally on a weekly schedule on desktops and servers in a timely and expeditious manner without requiring the end user to specifically request the update. • Installs security patches to servers and desktops in a timely and expeditious manner. Must follow the guideline set forth within the ISVM notice published by DHS ESOC.	SI-3
5.7.c	System owners develop and enforce procedures to ensure proper malware scanning of media prior to installation of primary hard drives, software with associated files, and other purchased products.	AC-20 SI-3
5.7.d	Introduction of any recorded media into the CBP information technology environment may be a source of malicious code contamination. Scan such media and verify its source before using it in the CBP environment.	SI-3
5.7.e	Only approved virus scanner-detection programs are used.	SI-3 SI-4
5.7.f	The LAN or System Administrator (SA) updates virus signature files as soon as possible after each new release is tested.	SI-3
5.7.g	All virus infections are immediately reported to the SOC and notify your supervisor/manager if it is a significant incident. This is critical to prevent further spread of the infection. (See DHS 4300A Attachment F, *Incident Response* for details.)	IR-1 IR-4 IR-5 IR-6
5.7.h	CBP may implement appropriate file/protocol/content filtering to protect their data and networks in accordance with their Internet usage policy.	AC-20 PL-4

5.7.1 What Is a Virus?

A virus is a self-replicating malicious program segment that attaches itself to legitimate applications programs, operating system commands, or other executable system components and spreads from one system to another. It can also be defined as a program or piece of code that is loaded onto a computer without the user's knowledge and runs against the user's wishes. As it spreads, it is said to be *infecting* the system.

A computer virus may only be a line or two of programming code hidden within a program. It can be benign and limited to sending a greeting to amuse or annoy, or malicious, written specifically to damage other programs. It can display a message, erase files, subtly alter stored data, or "crash" a hard drive.

5.7.2 Types of Malware

Various types of malware are defined in the following table:

Virus: A virus is a self-replicating malicious program segment that attaches itself to legitimate application programs, operating system commands, or other executable system elements and spreads from one system to another. Another definition for virus is: a program or piece of code that is loaded onto a computer without the user's knowledge and runs against the user's wishes. As it spreads, it is said to be *infecting* the system. **Worms:** Computer worms are malicious programs that copy themselves from system to system, rather than infiltrating legitimate files. For example, a mass-mailing email worm is a worm that sends copies of itself via email. A network worm makes copies of itself throughout a network or through file shares. Worms often contain Trojan horse or "backdoor" programs. **Logic Bombs:** A logic bomb can be defined as dormant code, the activation of which is triggered by a predetermined time or event. For example, a logic bomb might start erasing data files when the system clock reaches a certain date or when the application has been loaded X number of times. **Trojan Horses:** A Trojan horse is a computer program that is apparently or actually useful but performs another function. A Trojan horse generally provides remote control access to an unauthorized person. A Trojan horse can be used to modify databases, write checks, send email, or destroy files. It could be imbedded by a programmer or downloaded from the Internet. **Web Bugs:** A web bug is executable code included in an image (as small as one pixel) that can disrupt the operation of a system or acquire and transmit information from a system without the user's knowledge by merely visiting a malicious or compromised web site. **Backdoor:** A backdoor is a method of bypassing a system's security controls. The backdoor may take the form of an installed program or could be a modification to an existing program or hardware device.

5.7.3 How Malware Affects Systems

Regardless of the type of malicious code, malware poses a significant threat to CBP systems, which can affect the availability, integrity and confidentiality of information and processing resources. *Therefore, it is essential that all systems employ prevention measures commensurate with the level of risk identified in the risk analysis.* What makes malware unique is that it can spread from program to program and from system to system *without direct human intervention*. Systems that can be accessed by CBP-approved browser configurations should be categorized (trusted, untrusted, etc.). Users are not allowed to deploy Web browsers "out of the box," since the security policies implemented in such tools tend to reflect the vendor's interests and do not necessarily coincide with those of CBP.

5.7.4 Procedures When Malware Is Detected on a System

If malware/a virus or other malicious code is detected, the LAN/system administrator is responsible for taking appropriate actions to eradicate the problem. Such actions include:

- Running disinfectors available with antivirus software
- Scanning backup diskettes and tapes for malware/viruses prior to restoring system applications and data files
- Checking for re-infection from overlooked disks or other media during the eradication process
- Notifying the ISSO of the security incident via incident reporting procedures described in Section 4.9, *DHS and CBP Information Security Operations*.

Once the malicious code has been eradicated, the system administrator shall determine the extent of the damage and restore all damaged files or programs to uninfected files and programs. Back-up media should be scanned *prior to restoring* system applications and data files. Occurrence of malicious code constitute a *security incident* that must be reported; reporting procedures are described in Section 4.9.6, *Security Incidents and Incident Response and Reporting*.

Virus protection responsibilities are provided below:

Malware Protection Responsibilities
CISO • Establish and enforce malware protection control policy. • Provide technical expertise and evaluate the effectiveness of malware protection approaches. • Ensure that vulnerability to viruses and other malicious code is detailed in the risk analysis section of the Security Authorization documentation and that adequate steps to mitigate that risk are taken for each system. **System Owners** • Assess the impacts associated with system downtime caused by viruses and other malicious code and ensure adequate resources are allocated to address continuity of operations (CO).

Malware Protection Responsibilities
System/Network/LAN Administrators/FTOs • Ensure that all CBP systems employ malware protection software. • Ensure that malware protection software is installed on every workstation, network, laptop, and mobile computing device. • Update malware signature files immediately with each new release. • Ensure that malware protection software employs resident scanning. • Ensure that malware scanning occurs automatically during boot-up and installation of new software. • Ensure that all diskettes are scanned for viruses prior to use (including blank disks). • Follow procedures detailed in this manual in the event that a virus is detected. **ISSOs** • Employ malware prevention measures commensurate with the level of risk in the risk analysis. • Ensure that procedures are implemented to prevent, detect, eradicate, and report computer malware incidents. • Ensure that malware incidents are reported in accordance with SOC procedures (see Section 4.9, *DHS and CBP Information Security Operations*). **Users** • Ensure that no files are downloaded or opened from unknown or untrusted sources. All files should be scanned by malware detection software before opening them. • Do not open suspicious email. • Notify the System/Network Administrator if malware detection software is not installed on the user workstation. • Never disable malware detection software functions. • Report malware and other malicious code incidents in accordance with procedures described in Section 4.9.6, *Security Incidents and Incident Response and Reporting*.

5.8 Product Assurance

Information Assurance (IA) involves protecting and defending information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. Information assurance is achieved through the use of IA and IA-enabled products.

Policy ID	CBP Policy Statements	Relevant Controls
5.8.a	Information Assurance (IA) is considered a requirement for all systems used to input, process, store, display, or transmit sensitive or national security information. IA is achieved through the acquisition and appropriate implementation of evaluated or validated Commercial off-	---

Policy ID	CBP Policy Statements	Relevant Controls
	the-Shelf (COTS) IA and IA-enabled IT products. These products provide for the availability of systems. The products also ensure the integrity and confidentiality of information and the authentication and nonrepudiation of parties in electronic transactions.	
5.8.b	*Strong preference* is given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting sensitive information) that have been evaluated and validated, as appropriate, in accordance with the following: • The National Institute of Standards and Technology (NIST) FIPS validation program • The National Security Agency (NSA)/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program • The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement	---
5.8.c	The evaluation and validation of COTS IA and IA-enabled IT products are conducted by accredited commercial laboratories or by NIST.	---
5.8.d	CBP uses only cryptographic modules that have been validated in accordance with FIPS 140-2. Also, see Section 5.6, *Cryptography.*	---
5.8.e	Transaction-based systems (e.g. database management systems, transaction processing systems) implement transaction rollback and transaction journaling, or technical equivalents.	CP-10
5.8.f	For systems with moderate or high impact for the integrity security objective, CBP performs a risk-based analysis to determine any data inputs that are critical to the system mission or the correct handling of the security controls, which should be checked for accuracy, completeness, and validity of the information as close to the input point (e.g., user interface) as possible. Inputs that go through interpreters should be prescreened.	SI-10
5.8.g	For system with moderate or high impact for the integrity security objective, the information system checks the validity of the CBP defined information inputs.	SI-10
5.8.h	For systems with moderate or high impact for any of the FIPS 199 security objectives, CBP performs a risk-based analysis to determine what error conditions should be identified and how expeditiously they should be handled.	SI-11
5.8.i	For systems with moderate or high impact for any of the FIPS 199 security objectives, the information system generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. Error	SI-11

Policy ID	CBP Policy Statements	Relevant Controls
	messages are only revealed to authorized personnel.	

Product assurance responsibilities are provided below:

Product Assurance Responsibilities
CISO • Provide guidance in the use of Commercial off-the-shelf (COTS) information assurance products. **Security Control Assessors** • Validate the proper use of information assurance products. **System/Network Administrators/FTOs/ISSOs** • Ensure selected information assurance products are properly deployed and configured. **Project Managers** • Comply with product assurance policy during system development.

The National Information Assurance Partnership (NIAP), collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA), is a U.S. Government initiative designed to meet the security testing, evaluation, and assessment needs of both IT producers and consumers. NIAP combines the extensive security experience of both agencies to promote the development of technically sound security requirements for IT products and systems and appropriate metrics for evaluating those products and systems.

The NIAP Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS) is a partnership between the public and private sectors, to evaluate IT product conformance to international standards. This program is being implemented to help consumers' select COTS IT products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace.

CBP will be kept apprised of the above ongoing initiatives and strongly consider the recommendations and findings of the NIAP in the selection of COTS products. This guidance applies to both stand-alone COTS products as well as those incorporated in other IT systems.

Compliance with this policy, coupled with the restriction that the products have been appropriately validated by the designated Federal authorities and the Common Criteria, will reduce costs and remove the burden of maintaining and providing interoperability between numerous custom written software systems by a variety of contractors.

5.9 Supply Chain

Supply chain threats shall be considered during every sensitive system acquisition and throughout those systems' life cycle.

Policy ID	CBP Policy Statements	Relevant Controls
5.9.a	CBP assigns an impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability) for each DHS information system. CBP applies NIST SP 800-161 controls as tailored specifically to the security objective at the determined impact level.	SA-12
5.9.b	CBP implements NIST SP 800-161security controls, using the FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems methodology, based on the FIPS 199 impact level established for each separate security objective (confidentiality, integrity, availability).	SA-12

Both the public and private sectors generally recognize that much of the trustworthiness challenge facing commercial Information and Communications Technology (ICT), including hardware, software, and services, stems from decisions made by suppliers. Weaknesses exist in commercial ICT product development and in the underlying business systems that produce them, but more importantly, acquirers are accepting risks that result from these weaknesses on behalf of the end user without providing the information needed to assess the risk themselves. These supply chain weaknesses, and the costs of not reducing the consequent risks, become the burden of the end user.

CBP assigns an impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability) for each DHS information system, applying NIST SP 800-161 controls tailored specifically to the security objective at the determined impact level.
NIST SP 800-161security controls are implemented by use of the FIPS Pub 200, "Minimum Security Requirements for Federal Information and Information Systems" methodology, based on the FIPS 199 impact level established for each separate security objective (confidentiality, integrity, availability).

Supply chain risk mitigation activities can take place at any time during a system's lifecycle, but the opportunity to influence the trustworthiness of the system's commercial ICT products and services is greatest during acquisition and in preparation for milestone reviews. At these times, supplier business risks and rewards are greatest. Even procurements associated with operational support and system retirement offer an opportunity to mitigate supply chain risk. A strategy to manage supply chain risks must include the following actions:

1) Development and implementation of supply chain risk management strategies at the enterprise, component, division, department, and operational level of each system.
2) Education and training of DHS staff and contractors about supply chain risks, and about each person's role in managing that risk.

3) Enforcement of good DHS supply chain hygiene, and extension of this enforcement to suppliers by establishing contractual requirements and audit mechanisms to enforce those requirements.

Future policy revisions will integrate these actions into existing and new requirements, particularly with regard to accountability for identification and mitigation of supply chain risk. Opportunities for SCRM education and training, as well as for broad awareness of supply chain hygiene, will be the manifest response to the implementation of this strategy.

5.9.1 Business Impact

DHS depends on numerous external supply chains for the hardware, software, and services needed in order to accomplish its missions effectively. Many of these supply chains are independent of one-another and come with their own set of risks. All program risk owners need to make risk management decisions on how best to manage these risks. It is often no longer enough for acquisition staff to perform due diligence at the beginning of an acquisition. Effective supply chain risk management (SCRM) requires the analysis of the Business Impact

Assessment (BIA) to determine if supply chain threats represent unacceptable business or mission risk and the optimal countermeasures.

Policy ID	CBP Policy Statements	Relevant Controls
5.9.1.a	BIA is used to determine the level of risk introduced to the system by the IT supply chain and whether the IT supply chain threat introduces sufficient risk to require the implementation of countermeasures.	SA-12

A BIA is most effective at the point in the system acquisition and development lifecycle at which services, and the allocation of government and contractor responsibilities to determine the likelihood of harm to the enterprise.

5.9.2 Supply Chain Risk Management Plans

For the development of SCRM plans, no prescriptive set of mitigations can be provided; rather, it is necessary for organizations across DHS to consider the range of countermeasures which could be selected. It will be up to individual programs to establish the appropriate supply chain risk reduction strategies and determine the best way to implement them.

Policy ID	CBP Policy Statements	Relevant Controls
5.9.2.a	CBP develops, documents, and disseminates requirements for all programs under their control to develop a plan to address supply chain risk.	SA-1 SA-12
5.9.2.b	CBP assesses supply chain threats for risks associated with all	SA-12

Policy ID	CBP Policy Statements	Relevant Controls
	hardware, software, and services acquired or projected to be acquired with the goal of mitigating those risks to the greatest extent possible.	

All DHS organizations that acquire, develop, and operate sensitive systems require a SCRM Plan. There are three tiers of SCRM governance, two of which require SCRM plans:

- Tier 1: Governance as DHS Sensitive Systems Policy Directive 4300A, defining the SCRM policy for the DHS enterprise;
- Tier 2: SCRM plans that consist of a Component's specific guidance to mission and business owners who may supplement this component guidance as to the recommended controls and countermeasures;
- Tier 3: SCRM plans at the level of individual systems or programs, such plans either standing alone, or incorporated into the system's security plan.

These three SCRM governance tiers are shown in Figure 5.9.2.

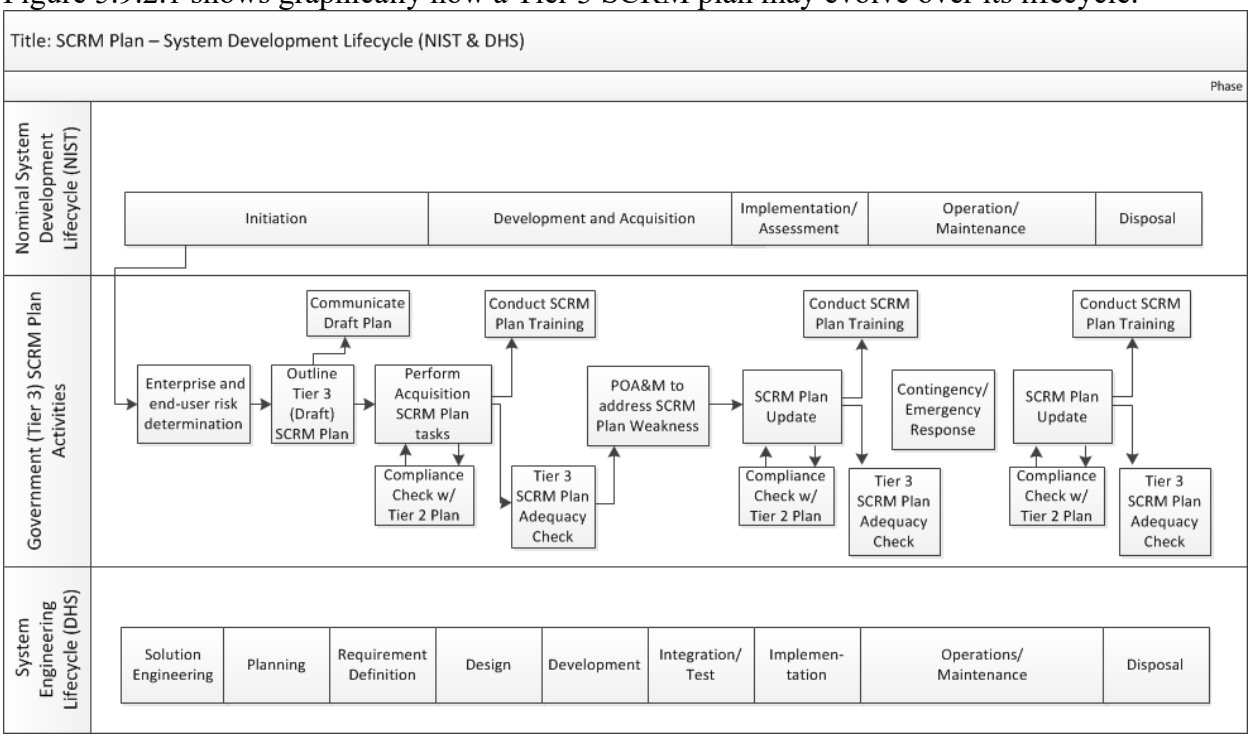
Figure 5.9.2. SCRM Plan Tiers

SCRM Plan Framework

SCRM plans should cover the full lifecycle of systems and programs, addressing acquisition, development, operations, sustainment, and termination or disposal. Plans should include, as attachments, relevant agreements provided by system integrators, suppliers, and external service providers as part of the contracting process. Such agreements, which can also be referred to as supplier SCRM Plans, may describe details of risk management activities performed on behalf of the end user by supply chain participants.

These agreements are typically reflected in plans submitted as a contractual deliverable and included in Tier 3 SCRM plans but may also be included in Tier 2 SCRM Plans for acquisitions that span multiple systems. Review and update SCRM Plans on a schedule that coincides with lifecycle milestones or control gate reviews and significant contracting activities.

Figure 5.9.2.1 shows graphically how a Tier 3 SCRM plan may evolve over its lifecycle.



SCRM Plan Sections

Structure of an SCRM Plan should have nine (9) numbered sections as given below.

1. Introduction

Describe the purpose of the SCRM Plan. Tier 2 Plans may need to be derived, in whole or in part, from existing policies or other guidance. Tier 3 Plans may be closely tied to or integrated with Security Plans (SP) but may also be retained as "stand-alone" documents in the case of, for example, legacy systems with no expected changes to existing documents. These systems still

require SCRM plans to ensure that supplies, replacement parts, support contracts, etc. comply with DHS Sensitive Systems Policy Directive 4300A.

For all tiers, provide a general statement that conveys the intent of the organizational leadership to adhere to the Plan, enforce its controls, and ensure it remains current.

2. Purpose and Scope

Include: The name of the Department, Agency, or Component for which this Plan applies. For Tier 2:

- State a unique identifier given to the mission or business. This may be the name of an acquisition program, an IT acquisition (e.g., one listed in an applicable OMB Exhibit 300), or any other designator that describes the scope of the SCRM Plan at Tier 2.
- Provide a brief explanation of what this mission or business encompasses, including a high-level summary of systems within the scope of the Plan.
- List all Tier 3 SCRM Plans and/or System Security Plans that are within the scope of the Tier 2 Plan.

For Tier 3, if creating a separate SCRM Plan, include a unique identifier and name given to the system. (For consideration: List all essential supporting systems and interfaces (such as network infrastructure) and their relevant SCRM data from their SCRM plans if such a plan exists. This provides the opportunity for the Component or Agency to find missing, overlapping, and redundant controls. At minimum, most if not all supporting systems will require replacements, supplies, and upgrades.)

3. Authority

Include: Authorities and references to relevant DHS and Component documents, such as policies, strategic plan(s), acquisition guidelines, processes, procedures, etc. Policies may include SCRM policy, security policy, acquisition policy, and any other policy applicable to the context of this SCRM Plan.

For Tier 2, include the applicable Tier 1 SCRM Plan title.

For Tier 3, include the applicable Tier 1 and Tier 2 SCRM Plan titles.

4. Audience

For all three tiers, include all Components that should be active participants or interested parties in this plan, and that should be using it to influence their activities. These may include legal, acquisition, IT security, supply chain and logistics, human resources, finance, etc.; specific individual roles such as CISOs, procurement personnel, program managers, etc., as appropriate.

5. Roles and Responsibilities

For all three tiers, identify by position those responsible for the Plan and identify the key contributors to SCRM.

a. Responsibility for the Plan

State the role and name of the individual or group responsible for the Plan.

- For Tier 2, an example may be Chief Information Officer (CIO), mission or business function manager, or Program Manager
- For Tier 3, this is the System Owner and, if integrated into the Security Plan, the Authorizing Official.

Include the name, title, organizational affiliation, address, email address, and phone number of each person.

b. Key Contributors

Identify key contributors to the Plan.

- For Tier 2, an example may be Acquisition/Contracting, Operations Manager, System Architect
- For Tier 3, an example may be Systems Engineer, Security Engineer, and Developer/Maintenance Engineer.

Include the name, title, organizational affiliation, address, email address, and phone number of each person.

6. SCRM Controls

List applicable (per tier) SCRM controls resulting from the Evaluation of Alternatives. Description of each control should include the following:

- Title and description
- How the SCRM control is being implemented, or planned to be implemented
- Applicable scoping guidance
- Tailoring decisions with justifications

For Tier 2, reference the applicable Tier 1 SCRM Plan that provides common controls.

For Tier 3, reference the applicable Tier 2 SCRM Plan that provides common controls.

7. Using and Revising SCRM Plan

SCRM Plans are living documents that must be updated and communicated to all appropriate individuals - government staff, contractors, and suppliers.

a. Communicating SCRM Plan

Describe processes by which this SCRM Plan will be communicated to other Tiers to ensure supply chain interdependencies are addressed. Examples include:

- Posting on appropriate portal(s)
- Communicating via email

        - Briefing appropriate individuals including those responsible for addressing deficiencies
    - Including information contained in the SCRM Plan in applicable training and outreach materials.

b. Revision and Improvement

Tiers 1 and 2 SCRM Plans should be reviewed, at a minimum, on an annual basis since changes to laws, policies, standards, guidelines, and controls are dynamic and evolving. At a minimum, review and update Tier 3 SCRM plans at lifecycle milestones, gate reviews, and significant contracting activities, and verify compliance with upper tier plans as appropriate.

State the required frequency for SCRM Plan reviews to consider updates. Define criteria that would trigger SCRM Plan revisions. These may include:

- Change of authorities that apply to the plan
- Change of policies that apply to the plan
- Significant SCRM events
- Introduction of new technologies
- SCRM plan shortcomings
- For Tiers 2 and 3, change in the governing SCRM plan for the Tiers above
- Change of scope
- Other Component -specific criteria

SCRM Plan owners can use an SCRM Plan of Action and Milestones (POA&M) to assess the impact of the changes and guide SCRM Plan revisions and to ensure that the updated Plan does not leave a gap in coverage from the previous version. Describe SCRM POA&M process and resolution steps.

c. Implementing and Assessing Effectiveness of SCRM Plan

Components should use their SCRM Plans during budgeting and planning processes, particularly with respect to acquisition and procurement activities. Operations staff who procure replacement parts and ancillary services and who may not be aware of the potential supply chain risks associated with such procurements must also adhere to applicable SCRM plans. Each tier's SCRM Plan should describe SCRM monitoring and enforcement activities (including auditing, if appropriate) applicable to the scope of each specific Plan.

If appropriate, SCRM Plan owners may decide to use qualitative or quantitative measures to support implementation of the Plan and to assess effectiveness of this implementation. If such measures are used, they should be stated in the Plan.

Supplier-provided plans associated with Tier 3 systems should be included if such plans are part of contractual agreements.

Describe general details about the use of the SCRM Plan, such as when to initiate collaboration with engineering and contracting activities, the condition under which an SCRM Plan audit is performed, and permissible steps to enforce the conditions of the SCRM Plan.

8. Use of SCRM Plans during Contingencies and Emergencies

This paragraph is optional. Components should decide whether to use it depending on mission criticality, applicable threats, and other factors.

In the event of contingency or emergency operations, the Component may need to bypass normal acquisition processes in the interest of mission continuity. Contracting activities that are not vetted using approved SCRM Plan processes introduce unknown risk to the enterprise.

When appropriate at Tier 1, 2, or 3, describe abbreviated acquisition procedures to be followed during contingencies and emergencies, such as the contact information for SCRM subject matter experts, who can provide advice in the absence of a formal tasking and approval.

For Tier 1, describe Component procedures and waiver processes.

For Tier 2, describe mission and business procedures and waiver processes in addition to those included in Tier 1.

For Tier 3, describe system-specific procedures and waiver processes in addition to those required by Tiers 1 and 2.

9. Attachments

For Tier 2, attach or provide links to applicable Tier 3 plans.

For Tier 3, attach or provide links to applicable plans for essential supporting systems.

For Tier 3, attach applicable contractual agreements or SCRM plans provided by contractors or suppliers.

No prescriptive set of mitigations can be provided; rather, it is necessary for all DHS organizations to consider the range of countermeasures that could be selected. Table 5.8-1 provides some general recommendations. It is up to individual Components to establish their appropriate supply chain risk reduction strategies and to determine the best ways to implement them.

	Enhancement of Existing Information Assurance Activities	SCRM-Unique
Programmatic	Enhance Information Assurance and Information Security Programs with SCRM • Include procurement, delivery, and storage systems • Enhance risk analysis to include supply chain elements	Apply SCRM Countermeasures • Require source diversity • Enhanced review of integrators/suppliers • Procure products only through manufacturer/vendor-

	• Enhance access control to include information sharing restrictions on integrators and suppliers • Enhance configuration management with identify of SCRM objects • Require technical diversity • Establish integrator/supplier security awareness and training.	approved distribution channels when such channels exist. Ensure integrators do the same. • Practice anonymous acquisition when acquirer identity is sensitive • All-at-once acquisition of components and spare parts • Limit time between purchase and delivery • Require integrators/suppliers test components • Require flaw detection and remediation • Require an independent witness for some testing • Require integrators/suppliers document testing • Recursive requirements for integrators/suppliers

Technical	Enhance Technical and Operational Countermeasures with SCRM • Enhanced access control for integrators/suppliers • Enhanced intrusion detection and response • Enhanced acceptance testing • Enhanced disposal requirements • Enhanced continuous monitoring • Enhanced ISCM to integrate data collection • Enhanced review of integrator/supplier procedures	Apply SCRM Countermeasures • Employ formal and accountable transit, storage, and delivery procedures • Limit transit and storage of critical components to trusted channels/services • Specify use of a code analyzer prior to compilation • Use code signatures • Use/specify tamper-proof or tamper-evident packaging • Enable forensic analysis in system/component design

Document Change Requests

Changes to the CBP 1400-05D may be requested by emailing cyber.training.policy@cbp.dhs.gov.

Questions and Comments

For clarification of CBP information security policies or procedures, contact cyber.training.policy@cbp.dhs.gov.

Definitions

Many of the terms used in this policy handbook are defined in DHS 4300A, as inherited policy. Additional terms which are specific to CBP policy are defined below:

Chief Financial Officer (CFO) Designated Financial Systems: CBP maintains systems defined by the DHS CFO as financial systems based on the Office of Management and Budget (OMB) Bulletin No. 06-03, Audit Requirements for Federal Financial Statements, and DHS Technical Guidance No. 03-06–Laws and Regulations, Cross Servicing Assertion, and Draft OMB Bulletin 01-02. The DHS CFO identifies financial systems subject to OMB A-123 and Internal Controls over Financial Reporting (ICOFR) requirements ("CFO designated financial systems"). These designated financial systems require additional management accountability and effective internal control over financial reporting. For CFO designated financial systems, additional CBP specific roles and responsibilities are summarized in the Responsibilities section. NOTE: The DHS CFO-designated financial systems require additional management accountability and effective internal control over financial reporting, as outlined in Section *DHS Chief Financial Officer – Designated Financial Systems*.

Foreign Intelligence Information: This type of information relates to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but does not include counterintelligence (CI) except for information on international terrorist activities.

General Support System (GSS): A general support system (GSS) is an interconnected set of information resources that share common functionality and are under the same direct management control. A GSS normally includes hardware, software, information, applications, communications, data and users. Examples of GSSs include local area networks (LAN), including smart terminals that support a branch office, Department-wide backbones, communications networks, and Departmental data processing centers including their operating systems and utilities.

Human User Account: A Human User Account is assigned to a specific user who is responsible for all actions taken with the account. It encompasses a username, logon credentials, security access levels, system access, disk access, and service/application access. Human User Accounts are defined by two (2) account types:

- Non Privileged User Account - Intended for a human to use to gain access to a particular system and system resources such as an email application. The distinction is that a Non Privileged User Account is used only by one person and the logon credentials are only known by that person which is a one-to-one relationship between the account and the person using it to access system resources.
- Privileged User Account - A privileged user account is similar to a non-privileged user account in that the relationship between human and account is one-to-one. The difference is that a privileged user account would have access rights or capabilities greater than that of the general user. For example, a privileged user account for an email application would have the ability to make changes within the email system (add a new user, delete an employee who retired, name change, etc.).

Non-Human User Account: Non-Human User Account provides various system functions or services for devices, human users, applications or controlling system functions. Non-Human User Accounts include the following account types:

- System Account - Used for machine-to-machine interfaces.
- Service Account - Used for machine accounts that provide application services which can be accessed by human accounts through vendor or internal developed applications. These accounts control common system files and services that can be divided between multiple online/offline users.
- Device Account - Allow a system to manage actual hardware connected to the system
- or network.
- Generic Account - Used to control functions between the application and the underlying operating system (Windows, Unix, Linux, Redhat, etc.). Generic accounts necessitate an operational or criticality need for mission accomplishment and would require the

approval of the CISO and the AO via formal policy waiver request and documented within the Security Plan.

- Robotic Process Automation (RPA) Service Accounts - RPA makes use of two types of automation bots: attended and unattended. Attended bots are deployed by the user and physical presence of the user is required for token authentication and initiation. Unattended bots, or Digital Workers, are deployed on a server or virtual machine, initiated by a scheduling tool, and do not require the physical presence of a user.
- Digital Worker Service Account - Used for unattended robots that are deployed on virtual machines (VM) within CBP Amazon Cloud East (CACE) environment and emulate human users without the physical presence of a user.
    - The use of a Digital Worker Service Account and automated process must be approved by the system owner and documented within the System Security Plan (SSP).
    - The unattended Digital Worker Service Account will be assigned to an existing CBP system and the SSP will be updated to include the account's purpose and the scope of information that will be processed by the unattended Digital Worker Service Account.

These accounts are exempt from logon credential policies. Exemptions must be specifically approved by the System Owner and documented in the System Security Plan and/or associated Security Design Document, based on mission criticality and system operability risk factors.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

Attachments

A – Foreign Service Nationals and Locally Employed Staff

C – Information System Security Officer (ISSO)

D – Type Accreditation

Q1 – Sensitive Wireless Systems

Q4 – Sensitive RFID Systems

Q5 – Voice Over Internet Protocol (VOIP)

Q6 – Bluetooth Security

R – Compliance Framework for CFO-Designated Systems

X – Social Media

Attachment A

Foreign Service Nationals and Locally Employed Staff

HB 1400-05D

INFORMATION SYSTEMS SECURITY POLICIES

Version 8.0

September 13, 2024

Introduction

CBP policy requires that only Government and contractor personnel who are U.S. citizens be granted access to CBP systems processing sensitive information. However, at times there is a need to grant access to non-U.S. citizens. The Commissioner or designee may grant access to CBP systems for non-CBP Government employees and/or non-U.S. citizens only when (1) the individual is a legal permanent resident of the United States or a citizen of any nation on the Allied Nations List maintained by the Department of State, (2) all required security forms specified by the Government and any necessary background check have been satisfactorily completed, (3) a compelling reason exists for using this individual instead of a U.S. citizen, (4) the exception to the U.S. citizenship requirement is in the best interest of the U.S. Government, and (5) the DHS Chief Security Officer and the Chief Information Officer or their designees concur in approving access for the individual.

Policies

Policy ID	CBP Policy Statement	Relevant Controls
4.1.1.c	CBP ensures that only U.S. Citizens are granted access to DHS/CBP systems and networks. Exceptions to the U.S. Citizenship requirement may be requested by submitting a completed Foreign National Access Request form for each foreign national to the CBP Foreign Access Coordinator at FSNREQUESTS@CBP.DHS.GOV.	PS-2
4.1.1.e	Non-CBP personnel who access CBP information systems and data (e.g., members of the trade community, local law enforcement, Department of State FSN/LES (See 4.1.1.3), or emergency response personnel) are identified. Access will be authorized through procedures that comply with CBP system access policies	PS-3 (3)
A-1	Any Person of dual citizenship (one being a U.S. citizenship), any Legal Permanent Resident and any individual hired through a Personal Services Contract who require access to DHS/CBP systems shall be processed as indicated in this attachment and in DHS 4300A, *Information Technology System Security Program, Sensitive Systems*.	PS-3
A-2	Exceptions to the U.S. Citizenship requirement are requested by submitting the completed required information and documents to the CBP Foreign Access Coordinator (FAC) for each FSN/LES requiring access to CBP systems and networks. The FAC will conduct a pre-systems access security review by which an FSN/LES	PS-3

	proposed access is evaluated. This security review will also address the issuance of CBP IT equipment, such as laptop and cellular telephone/mobile devices	
A-3	CBP requesting the issuance of DHS/CBP IT equipment to an FSN/LES will ensure the foreign national's citizenship is known and authorized to the servicing CBP CISO element.	
A-4	CBP CISO is the final authority concerning foreign access to CBP IT systems.	AC-1
A-5	DHS OCSO/CISS will require a Foreign Access Security Plan in cases where foreign nationals will have prolonged, continuous access to DHS/CBP systems and personnel, and will request an evaluation of the physical location of FSN/LES assignment for inadvertent exposure to other CBP/DHS systems or information they are not authorized to access.	PS-3
A-6	FSN/LES will be given a unique identifier (HASH ID) by the Foreign Access Coordinator.	
A-8	FSN/LES who are provided email access are identified by the "FSN" suffix in the email display name and the use of "@ForeignNational.cbp.dhs.gov" i.e., John.Doe@ForeignNational.cbp.dhs.gov, DOE, JOHN (FSN)	
A-9	FSN/LES nominated for access to CBP IT systems in a remote fashion, without being physically located in a CBP facility or co-located with CBP personnel (i.e. CBP Portals, etc.) will not be authorized.	

Procedures

Special procedures apply to request a waiver to the U.S. citizenship requirement. Access for FSN users is normally a long-term commitment, and waivers to citizenship requirements are treated differently from security policy waivers. Exceptions to the U.S. Citizenship requirement should be requested by contacting the Foreign Access Coordinator. CBP CISO has identified a Foreign Access Coordinator to be the point of contact to the DHS OCSO for processing requests for exception to the U.S. Citizenship policy requirement.

For further information regarding the citizenship waiver process, contact the CBP Foreign Access Coordinator at FSNREQUESTS@CBP.DHS.GOV

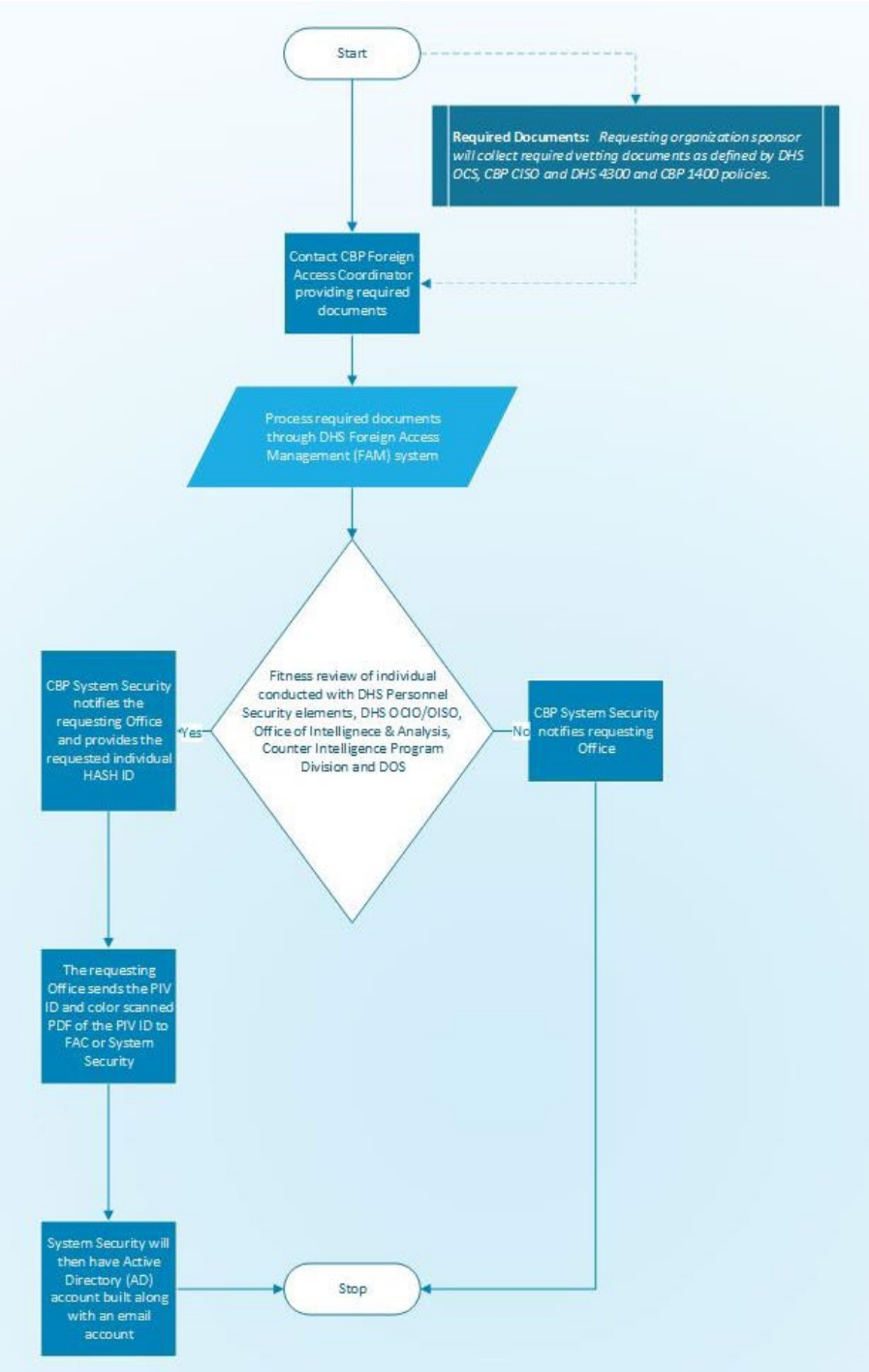
The CBP Foreign Access Coordinator will process the request through the DHS Foreign Access Management (FAM) system. A thorough fitness review of the individual will be conducted with DHS Personnel Security elements, the DHS OCIO/OCISO, Office of Intelligence & Analysis, Counterintelligence Program Division, and the Department of State (DOS). In the event that the fitness review results in derogatory information on the individual, CBP System Security will notify the requesting Office as appropriate.

Once a favorable determination on the individual's fitness review is completed, a User Access Request Form must be filled out at https://fsnlesuarequest.cbp.dhs.gov/FSNLESUAR/FSNUAR/. CBP System Security will then have an Active Directory (AD) account created. Once the individual receives their PIV ID Card, System Security will need the PIV ID number and a color PDF of the PIV ID Card. The issuance of a PIV Card, as well as the individual's access to DHS/CBP networks and systems, is dependent upon a favorable determination on the individual's fitness review. See the list below of documents required.

Required Documents for Vetting Foreign Service National (FSN), Locally Employed Staff (LES) and Personal Service Contracts:

- Individual's personal, active (unexpired) official, and/or diplomatic passport for all countries of citizenship (PDF scanned color copy)
- Diplomatic Badge
- DHS MD4900
- DHS 11000-6
- DHS 11059 (for first request only)
- Assistant Commissioners (AC) Memo from the requesting Office for limited access
- Fellowship program participants that work at the National Targeting Center (NTC) or Air and Marine Operations Center (AMOC) must provide a copy of the International Memorandum of Understanding in lieu of AC Memo
- Department Of State Regional Security Officer (RSO) signed current CBP CSD 7301FN-FSN Validation Form
- CBP FSN User Account Request Form (https://fsnlesuarequest.cbp.dhs.gov/FSNLESUAR/FSNUAR/Forms/AllItems.aspx)
- SF85P for U.S. citizens only
- Visa or Foreign Government document to live and work in the country
- Job position details
- Systems justification
- All other documents and information as required or requested

Vetting Process Flow Chart:



U.S. CUSTOMS AND BORDER PROTECTION

ATTACHMENT C

INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

HB 1400-05D

INFORMATION SYSTEMS SECURITY POLICIES AND PROCEDURES HANDBOOK

VERSION
7.0

NOVEMBER 16, 2017

THIS PAGE INTENTIONALLY BLANK

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	Updates reflecting changes from DHS in Section 1.0 removing stipulation that only waivers and exceptions for key controls must go to the CFO or Chief Privacy Officer first. Also formally updated the template to include signature lines for the Chief Privacy Officer and the Chief Financial Officer.
3.0	February 8, 2012	No revisions were made.
4.0	May 10, 2013	New request form design.
5.0	June 17, 2014	No Changes.
5.1	October 30, 2014	Revised form to remove exception requests.
6.0	March 3, 2016	No Changes.
6.01	May 17, 2016	No Changes.
6.02	September 2016	No Changes.
7.0	November 16, 2017	No Changes.

DHS Information Systems Security Officer (ISSO) / Alternate Information Systems Security Officer (AISSO) Designation

The following person is designated as the ☐ ISSO / ☐ AISSO for the _____ (major application or general support system, as appropriate)

Name	
DHS Component	
Title	
Office	
Telephone Number	
E-mail Address	

Affiliation (select one)

☐ DHS Employee.

☐ DHS Support Contractor. If support contractor, provide name of contracting company: _____

Clearance

☐ ISSO has been granted a Secret clearance (minimum)

Designating Official (System Owner, Senior Site Manager, or ISSO, as appropriate)

Name: _____ Title: _____

Signature: _____Date: _____

Review and Approval (by the Component Chief Information Security Officer or delegate)

Name: _____ Title: _____

Signature: _____ Date: _____

Comments: _____

ISSO / AISSO Acknowledgment of Responsibilities

I, _____ (print name), have been formally designated an ☐ Information Systems Security Officer (ISSO) / ☐ Alternate Information Systems Security Officer (AISSO) for the _____ (major application or general support system, as appropriate). I understand that I am responsible for coordinating information technology security regulations and requirements, as described in appropriate security policy publications and handbooks, including the following:

- Ensuring that security requirements for the major application or general support system with which I am involved are being or will be met.
- Ensuring that requests for certification and accreditation of computer systems are completed in accordance with the published procedures.
- Ensuring that protective measures such as deadbolt locks on doors, placement of electrical wiring, etc. as countermeasures for physical security threats, are in place.
- Ensuring compliance with all legal requirements concerning the use of commercial proprietary software, e.g. respecting copyrights and obtaining site licenses.
- Maintaining an inventory of hardware and software within the program and development offices or field site facility.
- Coordinating the development of a Contingency Plan and ensuring that the plan is tested and maintained.
- Ensuring that risk analyses are completed to determine cost-effective and essential safeguards.
- Ensuring preparation of security plans for sensitive systems and networks.
- Attending security awareness and related training programs and distributing security awareness information to the user community as appropriate.
- Reporting IT security incidents (including computer viruses) in accordance with established procedures.
- Reporting security incidents not involving IT resources to the appropriate security office.
- Providing input to appropriate IT security personnel for preparation of reports to higher authorities concerning sensitive and/or national security information systems.

DHS Component:
_____

Office: _____Telephone Number: _____

Signature _____ Date _____

U.S. CUSTOMS AND BORDER PROTECTION

ATTACHMENT D

TYPE ACCREDITATION

HB 1400-05D

INFORMATION SYSTEMS SECURITY POLICIES AND PROCEDURES HANDBOOK

VERSION
7.0

NOVEMBER 16, 2017

THIS PAGE INTENTIONALLY BLANK

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	NO CHANGES.
3.0	FEBRUARY 8, 2012	NO CHANGES.
4.0	MAY 10, 2013	EDITED FOR GRAMMAR AND STYLE.
5.0	JUNE 17, 2014	NO CHANGES.
5.1	OCTOBER 30, 2014	NO CHANGES.
6.0	MARCH 3, 2016	NO CHANGES.
6.01	MAY 17, 2016	NO CHANGES.
6.02	SEPTEMBER 2016	NO CHANGES.
7.0	NOVEMBER 16, 2017	NO CHANGES.

CONTENTS

1. INTRODUCTION 5

2. DEFINING BOUNDARIES FOR SYSTEMS WITH COMMON SECURITY CONTROLS 5

3. SECURITY AUTHORIZATION FOR SYSTEMS WITH COMMON SECURITY CONTROLS 6

4. MASTER SECURITY AUTHORIZATION PACKAGE 7

5. SITE-SPECIFIC CONSIDERATIONS 8

1. INTRODUCTION

TO STREAMLINE THE SECURITY AUTHORIZATION PROCESS, DHS COMPONENTS ARE ENCOURAGED WHEN POSSIBLE TO PURSUE TYPE ACCREDITATION. TYPE ACCREDITATION IS APPROPRIATE FOR A GENERAL SUPPORT SYSTEM (GSS) DEPLOYED AT MULTIPLE SITES BUT OPERATING IN A SPECIFIED ENVIRONMENT. FOR EXAMPLE, SEVERAL DHS ORGANIZATIONS PROVIDE SERVICES OVER LARGE DISTRIBUTED ENVIRONMENTS SUCH AS FIELD SITES AT AIRPORTS AND BORDER CROSSINGS. THESE FIELD SITES ARE EQUIPPED WITH REMOTE NETWORK CONNECTIONS, CLIENT-SERVER SOLUTIONS, AND OTHER RESOURCES, THAT MUST BE ACCREDITED FOR OPERATION, AND ACCOUNTED FOR IN DHS IT SECURITY RISK ANALYSES AND FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) REPORTS. THE COST TO INDEPENDENTLY EVALUATE AND ACCREDIT EACH OF THESE SITES IS PROHIBITIVE. A TYPE ACCREDITATION, HOWEVER, ALLOWS FOR CONSOLIDATING COMMON SECURITY CONTROLS ACROSS THE SITES AND FOR CONDUCTING A SINGLE MASTER SECURITY AUTHORIZATION. TO ACCOUNT FOR UNIQUE PHYSICAL AND LOGICAL VARIATIONS AT THE SITE LEVEL, A DESCRIPTION OF ANY DIFFERENCES AND THE ASSOCIATED RISKS AT EACH SITE ARE DOCUMENTED, AND THE SITE-SPECIFIC DOCUMENTS ARE INCORPORATED AS ATTACHMENTS OR APPENDICES TO THE MASTER SECURITY AUTHORIZATION PACKAGE.

2. DEFINING BOUNDARIES FOR SYSTEMS WITH COMMON SECURITY CONTROLS

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST SPECIAL PUBLICATION 800-37 (SP 80037) PROVIDES GUIDELINES FOR ESTABLISHING INFORMATION SYSTEM SECURITY BOUNDARIES. THE KEY GUIDELINES THAT NIST PROVIDES IN MAKING A BOUNDARY DETERMINATION INCLUDE:

1. THE INFORMATION RESOURCES SHOULD GENERALLY BE UNDER THE SAME DIRECT MANAGEMENT CONTROL. DIRECT MANAGEMENT CONTROL DOES NOT NECESSARILY IMPLY THAT THERE IS NO INTERVENING MANAGEMENT.
2. THE RESOURCES SHOULD HAVE THE SAME FUNCTION OR MISSION OBJECTIVE.
3. THE RESOURCES SHOULD HAVE OPERATING CHARACTERISTICS AND SECURITY NEEDS THAT ARE ESSENTIALLY THE SAME.
4. THE RESOURCES SHOULD RESIDE IN THE SAME GENERAL OPERATING ENVIRONMENT (OR IN THE CASE OF A DISTRIBUTED INFORMATION SYSTEM, THE RESOURCES SHOULD RESIDE IN LOCATIONS WITH SIMILAR OPERATING ENVIRONMENTS).

NIST SP 800-37 ALLOWS AGENCIES TO CENTRALLY MANAGE COMMON SECURITY CONTROLS IN A DISPERSED ENVIRONMENT. RELEVANT ATTRIBUTES FOR COMMON SECURITY CONTROLS ARE THE FOLLOWING:

1. COMMON SECURITY CONTROLS CAN APPLY TO A COMMON INFORMATION SYSTEM, SUBSYSTEM, OR APPLICATION (WHICH MAY INCLUDE COMMON HARDWARE, SOFTWARE, OR FIRMWARE) DEPLOYED AT MULTIPLE OPERATIONAL SITES.
2. THE DEVELOPMENT, IMPLEMENTATION, AND ASSESSMENT OF COMMON SECURITY CONTROLS CAN BE ASSIGNED TO RESPONSIBLE AGENCY OFFICIALS OR TO ORGANIZATIONAL ELEMENTS, BUT NOT TO INFORMATION SYSTEM OWNERS WHOSE SYSTEMS WILL IMPLEMENT OR USE THOSE COMMON SECURITY CONTROLS.

3. RESULTS FROM COMMON SECURITY CONTROLS ASSESSMENT CAN BE USED TO SUPPORT THE SECURITY AUTHORIZATION PROCESSES OF AGENCY INFORMATION SYSTEMS WHERE THOSE CONTROLS HAVE BEEN APPLIED.

ANOTHER GUIDELINE FOR DEFINING AN INFORMATION SYSTEM BOUNDARY WHEN COMMON SECURITY CONTROLS ARE IMPLEMENTED IS THE SECURITY CATEGORIZATION OF THE INDIVIDUAL INFORMATION RESOURCES AS DEFINED BY FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) PUBLICATION 199, "STANDARDS FOR SECURITY CATEGORIZATION OF FEDERAL INFORMATION AND INFORMATION SYSTEMS." THE RESOURCES MUST BE DEFINED TO OPERATE UNDER THE *SAME SECURITY CATEGORIZATION* (LOW, MODERATE, OR HIGH) FOR SELECTING A SET OF COMMON SECURITY CONTROLS.

PERHAPS MOST IMPORTANTLY, DHS REQUIRES THAT A SYSTEM SECURITY BOUNDARY MUST ENCOMPASS SYSTEM COMPONENTS THAT ARE GOVERNED BY A SINGLE POLICY AND ARE ACCREDITED BY A SINGLE AUTHORIZING OFFICIAL (AO). IF THE SYSTEM POLICY OR THE AO VARIES AT ANY OF THE SITES, FOR ANY OF THE DISTINCT SYSTEM COMPONENTS, OR FOR ANY OF THE INFORMATION RESIDING WITHIN THE BOUNDARY, THAT ENTITY (SITE OR SYSTEM COMPONENT) MUST BE PLACED WITHIN THE BOUNDARY OF ANOTHER SYSTEM OR AS AN INDEPENDENT SYSTEM.

USING THESE GUIDELINES, DHS COMPONENTS CAN DEFINE A SINGLE INFORMATION SYSTEM ENCOMPASSING OR PROVIDING SERVICES AT A NUMBER OF SITES.

3. SECURITY AUTHORIZATION FOR SYSTEMS WITH COMMON SECURITY CONTROLS

BY IDENTIFYING SYSTEM BOUNDARIES BASED ON THE NIST GUIDANCE AND DHS REQUIREMENTS STATED ABOVE, DHS WILL IMPLEMENT A MORE COST-EFFECTIVE APPROACH FOR PERFORMING ACCREDITATION ON MANY OF THE SYSTEMS DEPLOYED WITHIN THE DEPARTMENT. BY CONSOLIDATING COMMON CONTROLS AND CONDUCTING A SINGLE MASTER ACCREDITATION PACKAGE, THE EFFORT TOWARD A MASTER SECURITY AUTHORIZATION WILL BE REUSED AT EACH OF THE SITES. TO ACCOUNT FOR UNIQUE PHYSICAL AND LOGICAL VARIATIONS AT THE SITE LEVEL, A DESCRIPTION OF ANY DIFFERENCES AND THE ASSOCIATED RISKS AT EACH SITE MUST BE DOCUMENTED. THE SITE-SPECIFIC DOCUMENTS MUST BE INCORPORATED AS ATTACHMENTS OR APPENDICES TO THE MASTER SECURITY AUTHORIZATION PACKAGE.

THE SECURITY ASSESSMENT PROCESS IS THE COMPREHENSIVE ASSESSMENT OF THE MANAGEMENT, OPERATIONAL, AND TECHNICAL SECURITY CONTROLS IN AN INFORMATION SYSTEM. USING A COMMON CONTROLS APPROACH, THE ASSESSMENT PROCESS WILL EVALUATE TWO FACTORS:

1. CERTIFY THE MASTER SECURITY AUTHORIZATION PACKAGE DESCRIBING THE COMMON CONTROLS TO BE IMPLEMENTED ACROSS SITES.
2. CERTIFY THE DIFFERENCES FROM THE MASTER SECURITY AUTHORIZATION PACKAGE FOR THE PARTICULAR SITE. THIS INCLUDES A DEFINITION OF HOW CONTROLS AND ANY UNIQUE REQUIREMENTS HAVE BEEN IMPLEMENTED AT THE INDIVIDUAL SITES.

WITH A WELL-DESIGNED MASTER SECURITY AUTHORIZATION PACKAGE, THE UNIQUE SITE IMPLEMENTATIONS THAT NEED TO BE ADDRESSED DURING THE AUTHORIZATION PROCESS ARE MINIMIZED. THIS WILL ALSO MORE EFFECTIVELY CONTROL THE ENVIRONMENT AND SITE-SPECIFIC CHANGES.

THE SECURITY AUTHORIZATION PROCESS INCLUDES THE OFFICIAL MANAGEMENT DECISION GIVEN BY A SENIOR AGENCY OFFICIAL TO AUTHORIZE OPERATION OF AN INFORMATION SYSTEM AND TO EXPLICITLY ACCEPT THE RISK TO AGENCY OPERATIONS (INCLUDING MISSION, FUNCTIONS, IMAGE, OR REPUTATION), AGENCY ASSETS, OR INDIVIDUALS, BASED ON THE IMPLEMENTATION OF AN AGREED-UPON SET OF SECURITY CONTROLS. USING A COMMON CONTROLS APPROACH, THE PROCESS WILL EVALUATE THE RISKS AT THE "MASTER" LEVEL AND THEN EVALUATE ANY ADDITIONAL RISKS ASSOCIATED WITH PHYSICAL AND LOGICAL DEVIATIONS AT THE SITE LEVEL TO MAKE A SINGLE DECISION TO OPERATE FOR THE ENTIRE SYSTEM.

4. MASTER SECURITY AUTHORIZATION PACKAGE

THE MASTER SECURITY AUTHORIZATION PACKAGE (SAP) PACKAGE IS CRITICAL FOR A SUCCESSFUL DEPLOYMENT OF THIS TYPE OF ACCREDITATION. THE RESULTING AUTHORIZATION SHOULD BE SUFFICIENTLY ROBUST TO REPRESENT THE RISK ASSOCIATED WITH THE SYSTEM AND THE COMPLEX NATURE OF THE DEPLOYMENT. ADDITIONAL ATTENTION MUST BE PAID TO THE POSSIBLE SITE VARIATIONS AND COMPLEXITIES OF THE ENTIRE SYSTEM. THEREFORE, THE EFFORT AND COST ARE GENERALLY HIGHER THAN MOST TYPICAL ACCREDITATION PACKAGES.

WITHIN DHS, A MASTER SAP MUST INCLUDE THE FOLLOWING BASIC DOCUMENTS:

1. AN APPROVED SECURITY PLAN (SP)
2. A SECURITY ASSESSMENT REPORT (SAR)
3. A SECURITY ASSESSMENT PLAN (SAP)
4. A CONTINGENCY PLAN (CP)
5. A PLAN OF ACTION AND MILESTONES (POA&M) WHEN RISKS AND CONTROL WEAKNESSES HAVE BEEN IDENTIFIED
6. AN ACCREDITATION DECISION LETTER (ATO) SIGNED BY THE APPROPRIATE AO
7. SUPPORTING MATERIALS SUCH AS:
    - CONTINGENCY TEST PLAN RESULTS
    - FIPS 199 ASSESSMENT
    - PRIVACY IMPACT ASSESSMENT (PIA) STATEMENT
    - E-AUTHENTICATION STATEMENT
    - SELF-ASSESSMENT REPORT COMPLETED IN ACCORDANCE WITH NIST SP 800-53

[NOTE: DHS POLICY REQUIRES THE SAP CONTAIN ALL OF THE DOCUMENTS LISTED ABOVE AND THAT THEY BE UPLOADED INTO THE TRUSTED AGENT FISMA TOOL WHERE THEY BECOME SECURITY AUTHORIZATION "ARTIFACTS."]

THE ASSUMPTION FOR A SUCCESSFUL DEPLOYMENT IS A HIGH QUALITY MASTER PACKAGE, SPECIFICALLY DELINEATING SYSTEM CONTROLS TO A LEVEL OF DETAIL THAT ENABLES RECOGNITION AND DEFINITION BY THE SITE OF THEIR

DEVIATIONS FROM THE CONTROLS. SIGNIFICANT FINDINGS FOR THE MASTER SAP OR POOR QUALITY AND DETAIL SHOULD BE CONSIDERED TO BE AN EARLY INDICATION OF POOR RISK PLANNING AND SHOULD BE CONSIDERED BY THE AO IN MAKING ANY RISK-BASED DECISION. SITE-SPECIFIC MATERIAL

THE MASTER SECURITY AUTHORIZATION PACKAGE (SAP) PROVIDES AN UNDERSTANDING OF COMMON CONTROLS AND HOW THEY WILL BE IMPLEMENTED ACROSS THE DEPLOYMENT SITES. THE SITE-SPECIFIC MATERIALS DO NOT NEED TO ADDRESS CONSIDERATIONS ALREADY COVERED IN THE MASTER SAP, BUT EMPHASIS MUST BE PLACED ON ALL VARIANCES FROM THE COMMON CONTROLS AND ACTUAL SITE-SPECIFIC IMPLEMENTATION, CONFIGURATIONS, AND SYSTEM ENVIRONMENT, INCLUDING PHYSICAL ATTRIBUTES OF THE SYSTEM ENVIRONMENT AND ADMINISTRATIVE PROCEDURES SUPPORTING THE SYSTEM). EACH SITE WITHIN THE AUTHORIZATION BOUNDARY PROVIDES DOCUMENTATION THAT WILL BE USED TO SUPPORT THE SECURITY AUTHORIZATION OF THE ENTIRE SYSTEM. THE DOCUMENTATION CONTAINS TWO CRITICAL TYPES OF INFORMATION:

1. SITE-SPECIFIC DETAILS (FOR EXAMPLE DEVIATIONS FROM FUNCTIONALITY, CONFIGURATIONS, AND PHYSICAL CONTROLS)
2. SITE-SPECIFIC RISK ANALYSIS (FOR EXAMPLE ANALYSIS OF ADDITIONAL RISKS THAT RESULT FROM DEVIATIONS AT THE SITE)

THE EFFECTIVENESS OF THE SITE-SPECIFIC APPROACH IS DEPENDENT ON THREE FACTORS:

1. THE QUALITY OF THE MASTER SAP
2. THE CONFIGURATION MANAGEMENT PROCESS FOR IMPLEMENTING AND CONFIGURING NEW SITES
3. THE COMMUNICATION STRATEGY FOR ENSURING THAT SITES UNDERSTAND THE COMMON CONTROLS AND KNOW HOW TO PROPERLY IMPLEMENT AND CONFIGURE THEM

IN MAKING AN AUTHORIZATION DECISION, THE ORGANIZATION'S CHALLENGE IS IN DETERMINING HOW EFFECTIVELY THESE THREE FACTORS HAVE BEEN IMPLEMENTED.

AS PART OF THE SAR FOR EACH SITE, EMPHASIS SHOULD BE PLACED ON THE FOLLOWING KEY TOPICS SUPPORTING THE SITE IMPLEMENTATIONS:

1. CONFIGURATION MANAGEMENT AND CONTROL
2. COMMUNICATIONS WITH SITES
3. SITE-SPECIFIC DEVIATIONS FROM COMMON CONTROLS
4. SITE-SPECIFIC SECURITY IMPACT ANALYSIS

5. SITE-SPECIFIC CONSIDERATIONS

SOME SITE-SPECIFIC CONSIDERATIONS ARE THE FOLLOWING:

- **CONFIGURATION MANAGEMENT AND CONTROL.** BECAUSE EACH SITE HAS A UNIQUE OF COMMON CONTROLS IMPLEMENTATION, THE PROCESSES FOR MANAGING, CONTROLLING, AND DOCUMENTING INSTALLATIONS AND CHANGES FOR EACH SITE DEPLOYMENT IS CRITICAL TO SUCCESS. IT IS ESPECIALLY IMPORTANT THAT CONFIGURATION OF THE COMMON SECURITY CONTROL MECHANISMS BE STRICTLY CONTROLLED THROUGHOUT THIS PROCESS, AND THAT DEVIATIONS BE DOCUMENTED SO THAT RISKS ASSOCIATED WITH MODIFICATIONS CAN BE ASSESSED PRIOR TO AUTHORIZATION.
- **COMMUNICATION WITH SITES.** PERSONNEL AT EACH FIELD SITE ARE RESPONSIBLE FOR EFFECTIVELY IMPLEMENTING COMMON CONTROLS AS ELABORATED IN THE MASTER SAP. IN ORDER TO LOCALLY IMPLEMENT THE PLAN, SITES MUST BE AWARE OF AND MAINTAIN AN UNDERSTANDING OF THEIR RESPONSIBILITIES IN SUPPORT OF THE MASTER SAP. THEY WILL BEST ACHIEVE THE REQUISITE AWARENESS AND UNDERSTANDING THROUGH EFFECTIVE COMMUNICATIONS. KNOWLEDGE OF LOCAL CONTACTS, USER RESPONSIBILITIES, ESCALATION PROCEDURES, AND INCIDENT REPORTING PROCEDURES ARE SOME OF THE COMMON COMMUNICATION ISSUES THAT MUST BE CLEARLY DOCUMENTED FOR A SUCCESSFUL DEPLOYMENT. SITE INPUT AND ADHERENCE TO DOCUMENTED MASTER ADMINISTRATIVE PROCEDURES CAN ASSIST IN THIS COMMUNICATION.
- **SITE-SPECIFIC DEVIATIONS.** EACH SITE WILL HAVE UNIQUE REQUIREMENTS AND DESIGN CONSIDERATIONS. DEPENDING ON THE LEVEL OF THE MASTER SAP'S DETAIL, SITE-SPECIFIC DEVIATIONS MAY BE AS SIMPLE AS CREATION AND MAINTENANCE OF AN INSTALLATION CHECKLIST THAT RECORDS IMPLEMENTATION DETAILS (FOR EXAMPLE, LOCAL POINTS-OF-CONTACT (POC) AND INTERNET PROTOCOL (IP) ADDRESSES). ADDITIONALLY, SITE-SPECIFIC PROCEDURES AND INSTRUCTIONS (E.G., LOCATION OF BACKUP MEDIA AND STANDARD OPERATING PROCEDURES) MAY AUGMENT GENERAL ADMINISTRATIVE PROCEDURES FOR PERFORMING BACK-UPS AND FOR OTHER ROUTINE TASKS THAT ARE A PART OF THE MASTER SAP. ALL DEVIATIONS THAT COULD INFLUENCE POTENTIAL SYSTEM SECURITY RISKS MUST BE ACCOUNTED FOR IN SITE-SPECIFIC DOCUMENTATION. THIS IS ESPECIALLY TRUE FOR ANY SECURITY CONTROLS THAT ARE NOT IMPLEMENTED AT A PARTICULAR SITE (FOR EXAMPLE, PHYSICAL CONTROLS) BECAUSE THE MASTER SAP MAY BE DEPENDENT ON A CONTROL NOT IMPLEMENTED TO PREVENT EXPLOITATION OF SYSTEM VULNERABILITIES THAT ARE NOT OBVIOUS AT THE SITE LEVEL.
- **SITE-SPECIFIC SECURITY IMPACT ANALYSIS.** BASED ON SITE-SPECIFIC DEVIATIONS, AN IMPACT ANALYSIS MUST BE CONDUCTED TO DETERMINE IF ANY ADDITIONAL RISK HAS BEEN INTRODUCED TO THE OVERALL SYSTEM DUE TO SITE-SPECIFIC VARIATIONS. THIS ANALYSIS MUST BE PERFORMED AT THE MASTER LEVEL AND ALSO AT THE SITE LEVEL, SINCE VARIATIONS AT ONE SITE CAN AFFECT THE OVERALL SYSTEM POSTURE.

ADDITIONAL RISK MAY BE ADDRESSED BY REQUIRING A REVIEW OF THE COMMON CONTROLS SELECTED TO DETERMINE WHETHER THE RESIDUAL RISK HAS BEEN AFFECTED. ANY RESIDUAL RISK COULD POTENTIALLY RESULT IN DEVELOPMENT OF A POA&M FOR REMEDIATION AT THE SITE.

U.S. CUSTOMS AND BORDER PROTECTION

ATTACHMENT Q1

SENSITIVE WIRELESS SYSTEMS

HB 1400-05D

INFORMATION SYSTEMS SECURITY POLICIES AND PROCEDURES HANDBOOK

VERSION
7.0

NOVEMBER 16, 2017

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
3.0	February 8, 2012	No changes.
4.0	May 10, 2012	No changes.
5.0	June 17, 2014	No changes.
5.1	October 30, 2014	Rewritten as a new document to reflect new wireless technologies and security guidelines.
6.0	March 3, 2016	No Changes.
6.01	May 17, 2016	No Changes.
6.02	September 2016	No Changes.
7.0	November 16, 2017	No Changes.

Contents

1.0 INTRODUCTION 6
1.1 Purpose 6
1.2 Scope 7
1.3 References 7
2.0 SECURITY REQUIREMENTS FOR ALL WIRELESS SYSTEMS 9
2.1 Risk-Based Approach 9
2.2 Wireless System Threats and Countermeasures 10
2.3 Authentication 11
2.4 Confidentiality 11
2.5 Integrity 12
2.6 Management Control 12
2.7 Physical Security 12
2.8 National Information Assurance Partnership Common Criteria Security Validations ... 12
2.9 Logs 13
2.10 Configuration Controls 13
2.11 Software and Firmware Updates 13
2.12 Wireless Monitoring 14
2.13 Content Filtering 14
2.14 Traffic Separation 14
2.15 Security Assessment 15
2.16 Security Incident Response 15
2.17 Security Awareness Training 15
3.0 WLAN SECURITY GUIDELINE 16
3.1 Security Approach 16
3.2 Network Naming Conventions 16
3.3 ESSID Broadcasting 17
3.4 Access Control 17
3.5 Encryptions 17

3.6 WIDS 18
3.7 Wireless Intrusion Prevention Systems 18
3.8 Official Visitor Network 18
3.9 Perimeter Security 19
3.10 Radio Coverage and Power Level 19
4.0 FIXED ACCESS WIRELESS NETWORKS: SECURITY GUIDELINES 20
4.1 Bridge Link Confidentiality 20
4.2 Bridge Link Authentication 20
4.3 Bridge Radio Coverage Recommendations 20
5.0 WWAN: SECURITY GUIDELINES 21
5.1 WWAN Built-in Security Features 21
5.2 Private WWAN 23
5.3 Remote Access Through VPN Service 24
6.0 WIRELESS PERSONAL AREA NETWORKS: SECURITY GUIDELINES 25
6.1 Ad Hoc or Peer-to-Peer Networks 25
6.2 Devices 25
6.3 Coverage and Power Requirements 25
6.4 Bluetooth Device Communication Risks and Recommendations 25
6.5 Personal Identification Number Protection 25
6.6 Disabling Unwanted Profiles 26
6.7 Device Security Capabilities 26
7.0 INTEROPERABILITY 27
7.1 Interoperability governing body 27
7.2 Wireless System Interoperability 27
7.3 Wireless Standards 28
APPENDIX A – ACRONYMS 1
APPENDIX B – WLAN SYSTEM ARCHITECTURE 1
APPENDIX C – WIRELESS SYSTEM SECURITY CHECKLIST 3
APPENDIX D – WIRELESS SYSTEM RULES OF BEHAVIOR USER AGREEMENT 1

1.0 INTRODUCTION

Wireless communications technology enables exchange of information within a geographical area by encoding data into electromagnetic waves that propagate through space. The distances between communicating locations may be millimeters or thousands of kilometers. Wireless technologies utilize various portions of the electromagnetic spectrum, including radio frequency (RF) and infrared (IR), both analog and digital wave forms, and different types of encoding, including multiplexing, channel coding, modulation, and layered communication protocols. As technology evolves, new forms of wireless communications constantly emerge to meet the demands from governments, business communities, and consumers.

This document provides, from an information security perspective, techniques and procedures for implementing wide area, local area, and personal area wireless architectures for the Department of Homeland Security (DHS) information technology (IT) programs. Published as an attachment to the DHS 4300A Sensitive Systems Handbook, this document is the foundation for DHS Components to use in developing and implementing their wireless IT security programs. It is based on and considers statutes; Department directives and policies; guidance from the Government Accountability Office (GAO), the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), the Department of Defense (DoD), and national and international standardization organizations; and general wireless security best practices commonly recommended and followed by private industry and academic communities.

1.1 PURPOSE

This document is issued as implementation guidance for IT program managers and security personnel under the authority of the DHS Chief Information Officer (CIO) through the DHS Office of the Chief Information Security Officer (OCISO). This document addresses the security specifics of sensitive wireless systems only and does not cover the use of classified wireless systems. In accordance with *DHS Sensitive Systems Policy Directive (PD) 4300A*, the use of wireless communications technologies is prohibited within DHS unless the technology and the application are specifically approved by the appropriate Authorizing Official (AO). (In accordance with NIST Special Publication (SP) 800-37, the term *Authorizing Official* replaces the term *Designated Accrediting Authority* (DAA). AOs must also approve the implementation and use of wireless systems at a specified risk level during the certification and accreditation (C&A) process and ensure that appropriate and effective security measures are included in the security plan.

Given the ongoing rapid evolution in wireless technology, including different technology standards and multiple vendors' product offerings, specific wireless systems may or may not have the ability to be made wholly compliant with the countermeasures this document outlines. The guidelines set forth in this document are not intended to prohibit the use of

systems that cannot meet the countermeasures recommended herein; the intent, rather, is to provide a detailed explanation of potential wireless vulnerabilities and practical countermeasures in order for the Components to perform risk analysis and make an informed decision. AOs should pay particular attention to the potential risks that must be considered in approving wireless systems with technological barriers that prevent the adoption of these countermeasures. AOs should ensure that they understand the risks associated with a particular wireless system. This may include applying some but not all of the outlined countermeasures, as long as the risk is measured and mitigated to an acceptable level determined by the AO.

1.2 SCOPE

Wireless networks covered under this document include Wireless Local Area Networks (WLAN), wireless Wide Area Networks (WWAN), Wireless Personal Area Networks (WPAN), peer-to-peer wireless networks (i.e., ad hoc wireless networks), as well as wireless infrastructure that leverages commercial wireless services. Wireless systems include the transmission medium, stationary integrated devices, device firmware, supporting services, and communication protocols. Security policies and guidelines for wireless devices such as smart phones will be addressed in a separated document due to the complexity and rapid technology development in this area. *DHS Sensitive Systems Policy Directive 4300A* establishes the Department's wireless systems policies and general guidelines pertaining to all wireless communications technologies.

It should be noted that, with very few exceptions, almost all wireless systems are eventually connected to data packet-based wired networks that are managed by either DHS or outside third parties. While the security policies of wired networks are out of the scope of this document, the guidelines set forth in this document will address end-to-end as well as interface security requirements when both wireless and wired networks are involved.

The scope and contents of this document will change over time as new capabilities are added to DHS systems, as security standards are upgraded or created, and as a result of user experiences and comments. As the DHS IT wireless security programs mature, additional attachments to the DHS 4300A Sensitive Systems Handbook that address specific areas of security interest will be developed and published.

1.3 REFERENCES

The following documents were reviewed and referenced for this document:

- DHS, DHS Sensitive Systems Policy Directive 4300A, Version 9.1, July, 2012.
- DHS, Wireless Local Area Network Security Reference Architecture, Version 1.0, September 19, 2011.
- GAO, Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk, November 2010.

- NIST SP 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009.
- NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, February 2007.
- NSA, Guidelines for the Development and Evaluation of IEEE 802.11 Intrusion Detection Systems (IDS), Version 1.1, November 2005.
- DoD 8420.01, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies, November 3, 2009.
- IEEE, IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE-SA, June 12, 2007.
- IEEE, IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements, July 23, 2004.
- NIST SP 800-121, Guide to Bluetooth Security, June 2012.
- Wi-Fi Alliance, the State of Wi-Fi Security, January 2012.

2.0 SECURITY REQUIREMENTS FOR ALL WIRELESS SYSTEMS

The wireless security requirements listed in this section consist of a common set of core security capabilities and features that are applied to all wireless technologies. Requirements unique to specific types of wireless systems (e.g., 802.11 WLAN) will be addressed in the subsequent sections. As mentioned earlier, these requirements are derived from DHS directives and policies, guidance from other government sources, and practices recommended and followed by private industry, academic communities, and standardization organizations.

2.1 RISK-BASED APPROACH

A risk-based approach to wireless system security is a system-engineering approach to identify, assess, and prioritize risks associated with wireless systems and determine the likelihood and potential impact of these risks. Mitigation strategies and resources are then applied in defending against the most significant threats and preventing the incurrence of undue risks. For instance, unauthorized access points or devices on the DHS internal network occur sometimes and they pose great threat to the DHS information security as the internal network is regarded as trusted and within the defense perimeter. One mitigation strategy against this threat is to deploy effective detection and prevention tools to identify these threats and block their access when detected.

- A risk-based approach shall be used to mitigate risks associated with wireless systems.

At the highest level, two security classifications can be used to help identify and assess risks associated with a given wireless system:

- Trusted: Any combination of people, information resources, data systems, and networks that are subject to a shared security policy (a set of rules governing access to data and services). A trusted wireless system is within the accreditation boundary established by DHS and over which DHS has direct control for the application of required security controls or the assessment of security control effectiveness.
- Untrusted: Any combination that is outside the “trusted.” An untrusted wireless system is outside the accreditation boundary established by DHS and over which DHS has no direct control for the application of required security controls or the assessment of security control effectiveness.

Commercial or official visitor wireless networks, for example, should be considered untrusted because they are outside DHS control. DHS internal wireless networks are considered trusted because DHS can apply rigorous security policies and controls on these networks. Risks can be identified from the technology, process, and people perspectives by taking into account of the unique open nature of wireless systems and the rapid evolution of wireless technologies. The following section describes various wireless system threats and corresponding countermeasures in detail.

2.2 Wireless System Threats and Countermeasures

Wireless systems have their inherent weakness and vulnerabilities due to the open nature of wireless technologies, and security threats are widespread through a wide variety of attack methods. Wireless communications are susceptible to interference, eavesdropping, RF jamming, as well as threats typical to wired networks.

Threat Category	Description
Denial of Service	Attacker prevents or prohibits the normal use or management of networks or network devices.
Eavesdropping	Attacker passively monitors network communications for data, including authentication credentials.
Man-in-the-Middle	Attacker actively intercepts the path of communications between two legitimate parties, thereby obtaining authentication credentials and data. Attacker can then masquerade as a legitimate party. In the context of wireless systems, a man-in-the-middle attack can be achieved through a bogus or rogue Access Point (AP), which looks like an authorized AP to legitimate parties.
Masquerading	Attacker impersonates an authorized user and gains certain unauthorized privileges.
Message Modification	Attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
Message Replay	Attacker passively monitors transmissions and retransmits messages, acting as if the attacker were a legitimate user.
Traffic Analysis	Attacker passively monitors transmissions to identify communication patterns and participants, and extracts sensitive information.

Table 1. Wireless System Threats

Wireless system security addresses data confidentiality and integrity, authentication and access control, intrusion detection and prevention, logging and monitoring, as well as system availability and performance. The goal of wireless system security can be better achieved and the threats mitigated by adhering to federally-mandated standards and industry's information security best practices.

OSI Layer	Security Considerations
Application	Detect and prevent malicious code, viruses, phishing, and other malware applications. Mitigation tools include firewalls, anti-virus/malware detection software, Web security, and intrusion detection applications.
Presentation	Protect data files by cryptography (e.g., file password encryption).
Session	Protect system from port exploits or session hijacking. Use Secure Socket Layer (SSL) for Session and Transport layers.

OSI Layer	Security Considerations
Transport	Provide authentication and secure end-to-end communications such as the Secure Shell (SSH-2) protocol.
Network	Protect the routing and the forwarding protocols by robust authentication and encryption of routing data. The Internet Protocol Security (IPSec) standard provides meshed and simultaneous tunnels for secure communication.
Data Link	Protect the Media Access Control (MAC) sublayer from masquerade, DoS, impersonation, and Address Resolution Protocol (ARP) threats. Wireless protocols have built-in security features such as Layer 2 tunnels and message integration check.
Physical	Detect and prevent jamming and denial of service (DoS) attacks in the air medium via wireless intrusion detection system and intrusion prevention system (WIDS/IPS), which can detect abnormal signals and physically geolocate the suspicious devices via direction findings triangulation and timing algorithms. Employ anti-jamming techniques such as spread spectrum techniques.

Table 2. OSI Security Considerations

2.3 AUTHENTICATION

Authentication methods include IEEE 802.1X port-based network access control, Extensible Authentication Protocol–Transport Layer Security (EAP-TLS) authentication, and enterprise Remote (RADIUS) servers to provide mutual authentication to user devices and systems while providing for dynamic key management.

It should be noted that EAP-TLS requires existing Public-key Infrastructure (PKI). If a full-fledged PKI is not available, other authentication protocols, such as EAP-Protected Extensible Authentication Protocol (EAP-PEAP), can be used. These protocols only require a server side x.509 digital certificate that can be purchased from a third-party Certificate Authority, or a digital certificate can be issued from an organization's internal Certificate Authority. No user device authentication is provided in this case. Additional network control accesses, such as two-factor authentication, may be required to authenticate users and devices to ensure that they do not introduce security vulnerabilities and risks.

2.4 CONFIDENTIALITY

DHS PD 4300A requires that “Components shall use only cryptographic modules that are Federal Information Processing Standard (FIPS) 197 (Advanced Encryption Standard [AES]-256) compliant and have received FIPS 140-2 validation at the level appropriate to their intended use.”

2.5 INTEGRITY

Wireless traffic integrity is essential to ensure that data has not been modified in transit or at rest, and it also protects against other threats such as man-in-the-middle attacks. If a mechanism is available that allows for cryptographic verification of message integrity, system nodes must discard all messages that cannot be verified.

2.6 MANAGEMENT CONTROL

Wireless systems must be capable of supporting remote device management, establishment or change to configurations to comply with security policy, and updates of software and firmware. Wireless systems must have the ability to manage wireless infrastructure via management interfaces and tools which are part of the overall enterprise management infrastructure.

The network segment for management control should be integrated into the enterprise wired network, and it should be isolated from data networks to ensure robust management control. Security protections must not degrade or impede critical services or usability features protected by law or published policy (for example, compliance with Section 508 of the U.S. Rehabilitation Act).

A centralized wireless management structure provides a more effective means to manage the wireless infrastructure and the information security program as a whole. A centralized structure can also facilitate the development and implementation of standardized guidance, which allows organizations to consistently apply information security policies.

Wireless devices and/or software must not degrade or circumvent established system security controls. Any system modifications require appropriate security review and follow change management policies and procedures. In addition, configuration management and secure baseline configurations should be addressed in the organization's system security plan for that system.

2.7 PHYSICAL SECURITY

Routine inspections and surveillance for suspicious behavior will reduce the likelihood of unauthorized equipment operation and theft. Because wireless systems are susceptible to eavesdropping from a distance, guards and users alike should report to appropriate security personnel any suspicious individuals or activities in or around the facility.

2.8 NATIONAL INFORMATION ASSURANCE PARTNERSHIP COMMON CRITERIA SECURITY VALIDATIONS

The National Information Assurance Partnership (NIAP) is a U.S. Government initiative to address IT system and product security testing demands of both IT consumers and producers. NIAP is a collaboration of NIST and NSA to add a level of trust in IT products and networks. The Common Criteria define a set of validated IT requirements that can be used in establishing security requirements for products and systems. The Common Criteria also define Protection

Profiles (PP), or implementation-independent standardized sets of security requirements based on particular needs. PPs are available for products within the wireless security architecture. Additionally, a Security Target (ST) can be developed to measure security threats, objectives requirements, and summary specifications of security functions. STs are developed for specific products with specifically identified targets of evaluation. The STs may or may not conform to PPs to form a basis for evaluation.

When avoiding the use of processes that send clear text passwords or otherwise do not use a secure protocol (e.g., Telnet, HyperText Transport Protocol [HTTP], Simple Network Management Protocol [SNMP] v1/2, and Cisco Discovery Protocol [CDP]), for in-band device management, a possible secure configuration is to encapsulate insecure protocols inside encrypted tunnels; examples include IPSec and SSL-based Virtual Private Network (VPN).

2.9 LOGS

Logs serve as part of the wireless network monitoring and management capabilities to ensure that wireless networks are constantly monitored. They provide a traceable mechanism to record network activities and discover network intrusions. The integrity of logs should be protected by synchronizing the time clocks on all devices, remotely recording wireless activities and events, and enforcing strict access control for logs.

2.10 CONFIGURATION CONTROLS

Establishing configuration requirements and secure baseline configurations for wireless networks and devices can help ensure they are deployed in a secure manner in accordance with DHS security policies.

Wireless systems are usually initially configured with default vendor settings that are common knowledge. These settings can include network information such as default channel or modulation specification; security information such as network name, encryption methods, pass phrases or keys; and systems management information such as administration usernames, passwords, management port numbers, and default application services running.

2.11 SOFTWARE AND FIRMWARE UPDATES

The NIST National Vulnerability Database (NVD) "…is a comprehensive cybersecurity vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources."[1] When possible, the updated firmware should be tested in a nonproduction environment to validate functionality before a production rollout. System audit policy and guidance is provided in *DHS Sensitive Systems Policy Directive 4300A* and the DHS 4300A Sensitive Systems Handbook.

[1] http://nvd.nist.gov

2.12 WIRELESS MONITORING

Wireless monitoring capabilities include tools and methods for (a) conducting site surveys and the appropriate position of antennas to minimize signal leakage, (b) detecting misconfigured clients and using policy driven software or hardware solutions to ensure client devices and users comply with defined DHS wireless security policies, and (c) detecting and blocking suspicious or unauthorized activity or sources of radio interference.

Wireless intrusion detection systems (WIDS)/intrusion prevention systems (IPS) can detect network anomalies and monitor wireless infrastructure. Anomalies may include, but are not limited to, interference sources, abnormally high or low utilization, multiple login attempts, attack signatures, off-hour logins, and other suspicious variances from the system baseline.

2.13 CONTENT FILTERING

Content filtering is the process of monitoring communications such as email and Web pages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users. A dedicated server can be used to perform the content filtering task. For wireless systems that are internal to the organization wired networks, there are no specific requirements associated with content filtering that is already applied to the wired networks. Content filtering for external wireless systems such as visitor WLAN may be different than those applied on the organization's internal networks. Traffic from this network is not inspected by the National Cyber Protection System (NCPS), also known as Einstein. Therefore, organizations should define separated security controls for this network, such as allowing normal client connections via HTTP, Secure HTTP (HTTPS), and Domain Name Service (DNS) to only access limited Internet sites. In addition, the existing Trusted Internet Connections (TIC) capability can be leveraged to protect and monitor these external wireless systems.

All content filtering products must be kept up-to-date to ensure that their detection is as accurate as possible. Another key feature of content filtering packages is the scanning of inbound and outbound data for suspicious activities and taking preventive actions accordingly.

2.14 TRAFFIC SEPARATION

Traffic from different network segments may come from different security trust boundaries. For instance, official visitor wireless networks cannot be totally controlled by DHS (e.g., official visitor personal devices), so they introduce potentially serious security risks. As such, official visitor wireless traffic should be separated from the enterprise traffic via logical and/or physical means (e.g., IPSec tunnels or separated network circuits). Therefore, official visitors are only allowed to connect to the Internet and never access DHS enterprise resources.

2.15 SECURITY ASSESSMENT

Regular security assessments should be performed to evaluate the security posture of wireless networks and determine corrective actions needed to ensure that the wireless networks remain secure. Regular assessments help to determine whether wireless systems are transmitting correctly and are on the correct channels. Assessments can help Components determine whether controls are appropriately designed and operating effectively to achieve the organization's control objectives. The DHS 4300A Sensitive Systems Handbook describes the assessment areas and procedures in great detail.

2.16 SECURITY INCIDENT RESPONSE

Most security controls are designed to protect an organization against security threats; regardless of how effective those controls are, some security incidents are inevitable, and organizations need to have an effective response capability in place before they occur.

2.17 SECURITY AWARENESS TRAINING

Security awareness training is a fundamental part of information security to ensure that wireless networks are configured, operated, and used in a secure and appropriate manner. For security policies to be effective, those who are expected to comply with them must be aware of the policies. Additionally, the Federal Information Security Management Act (FISMA) mandates that agencies provide security awareness training for their personnel, including contractors and other users of information systems, that support the operations and assets of the agency. NIST recommends that security awareness training include the risks of wireless security and how to protect against those risks. The goal of security awareness training is to protect the confidentiality, integrity, and availability of DHS IT assets and data.

3.0 WLAN SECURITY GUIDELINE

The security guideline outlined in this section is developed to ensure robust design and implementation of WLAN systems. Appendix B describes the key components of WLAN infrastructure and their functionalities and provides a high-level WLAN system architecture.

3.1 SECURITY APPROACH

WLAN security specification is addressed by the IEEE 802.11i standard that provides security mechanisms against various WLAN security threats. The Wi-Fi Alliance, an international WLAN interoperability-advocate association, introduced Wireless Protected Access 2 (WPA2)—the interoperability certification for 802.11i implementation.

It should be noted that the 802.11i security standard only addresses WLAN security at OSI Layer 2. Layer 2 security methods address wireless authentication, frame encryption, message integrity check, and other security features. Use of Layer 2 security technology (IEEE 802.11i) does not preclude the use of defense-in-depth protection at other layers, including support for Layer 3 or higher security technologies, such as a VPN solution or application firewall. The strategy of multiple-layer defense helps to protect the wireless system from a number of individual attacks, thus raising the cost and complexity to potential attackers.

It is extremely important to understand one security deficiency associated with 802.11i security features: the management frames in 802.11 WLAN, such as authentication, association, beacon, and probe, are not protected. Therefore, WLAN is vulnerable to attacks associated with this deficiency, such as the DoS attack of bogus association requests. Security measures at higher layers, as well as the deployment of WIDS/IPS can mitigate this risk to a great degree. New security standard 802.11w addresses the protection of management frames, and this new security enhancement was added into the WPA2 implementation in 2012. However, support of the 802.11w standard among wireless devices is very limited.

3.2 NETWORK NAMING CONVENTIONS

WLAN contains a network name that identifies the network to client devices. In 802.11-based WLAN networks, this name is referred to as the Extended Service Set Identifier (ESSID). It is difficult to keep this network name a secret (i.e., known only by valid users) because it is transmitted unencrypted as a part of protocol management messages and can easily be intercepted by attackers. The ESSID name can be masked so that it does not reveal its affiliation to DHS operations or organizations or it is not associated with organizational function or identity to avoid advertising the network's identity or function to potential attackers. On the other hand, attackers may advertise false "Authorized DHS Wireless Service" and lure users to reveal their logon credentials through the fake wireless service, which is equally as dangerous as revealing the identity of the WLAN service through the explicit ESSID.

3.3 ESSID BROADCASTING

In some physical environments or operational areas, disabling the ESSID in broadcast beacons is important, so the existence of a WLAN is not advertised in the coverage area to mitigate the war-driving threat. War-driving is the act of driving, walking, or flying within a geographical area while employing wireless equipment to detect the presence of WLANs and attempting to map the locations in which these networks are discovered. Disabling the ESSID in the beacons prevents advertisement of the private WLAN to war-driving software tools and can help limit attackers' awareness.

An attacker listening for probed request and response packets can still capture a WLAN ESSID, but typically, this information is collected by determined hackers rather than those who pass by while conducting a war-drive. Therefore, it is essential to understand that disabling ESSID broadcasting only provides very limited deterrence to potential attackers but could cause inconvenience to end users and result in connection issues with some devices. It is important for organizations to understand the ESSID broadcasting mechanism and possible operation consequences and make an informed and balanced decision from both operation and security perspectives.

3.4 ACCESS CONTROL

Authentication and authorization can be enforced on WLANs by using 802.1X port-based access control and EAP authentication methods. These technologies combine to ensure that access is provided only to clients who have supplied valid credentials. Many EAP implementations exist for WLANs and are being incorporated into WPA2 interoperability certification processes.

Other network access control or Network Admission Control (NAC) solutions should be evaluated and deployed to ensure that only authorized devices are permitted network access, and risk based decisions should be implemented on hosts based upon their DHS or Component risk profiles. For example, DHS enterprise resource access is granted for DHS-issued devices only if they comply with antivirus and patch mandates; authorized visitor devices are only allowed to access the Internet.

Identity access management systems are needed to effectively operate WLANs. RADIUS, which was originally designed to support remote dial-in users, has been adapted to support WLAN authentication. RADIUS often has built-in support for Microsoft Active Directory (AD), Novell Directory Service (NDS), Windows Domain Authentication, Lightweight Directory Access Protocol (LDAP), and other identification and authentication databases.

3.5 ENCRYPTIONS

A properly configured WLAN should use the strongest end-to-end encryption mechanisms available to protect the confidentiality of traffic traveling across wireless links. The IEEE 802.11i security standard and its implementation WPA2 rely on the AES encryption algorithm for

confidentiality and integrity services.

DHS Sensitive Systems Policy Directive 4300A requires that "Components shall use only cryptographic modules that are FIPS 197 (AES-256) compliant and have received FIPS 140-2 validation at the level appropriate to their intended use." Non-standard systems require a CISO waiver and exemption approval.

3.6 WIDS

WIDS incorporate remote sensors that listen to airwaves and report findings to management appliances. These systems can detect malicious activities such as installation of unauthorized wireless hardware, access point (AP) outages, wireless client device hijacking, DoS attacks, unauthorized ad hoc or peer-to-peer networks, and other WLAN-specific vulnerabilities.

Signature-based WIDS scan for known attack signatures and are only as good as their latest signature update; therefore, they should be updated regularly. Although signature-based WIDS systems are not highly effective against new or zero-day attacks, they actively defend against known vulnerabilities and generate very few false-positives (also known as false alarms). Another complementary approach is anomaly detection. Anomaly detection operates by comparing the current system against the system baseline. Anomaly-based WIDS is more effective against new attacks than signature-based WIDS but places a large demand for system resources on the WIDS management appliance. In addition, anomaly-based WIDS produce more false positives than signature-based WIDS.

WIDS can perform troubleshooting, traffic and interference analysis, and unauthorized device detection to identify non-WLAN devices that operate in the same frequency bands, e.g., Bluetooth devices, cordless telephones, and microwave sources of interference. NSA published a detailed document to address the WIDS capability requirements and deployment best practices.[2] A key WIDS capability is the ability to provide, using triangulation or timing algorithms, physical location information on attackers, rogue devices, and other threats.

3.7 Wireless Intrusion Prevention Systems

Wireless intrusion prevention systems (WIPS) with active countermeasure capabilities are emerging within the WLAN industry. Such systems can actively deny service to suspected intruders, quarantine suspected intruders to benign segments of the network, and even perform active forensics on a suspected intruder to learn about the intruder's identity, methods, and goals.

3.8 Official Visitor Network

Official visitors (interns, short-term contractors, and people on official business) need to access the Internet, and they often use VPN technology to connect securely back to their own

[2] NSA, "Guidelines for the Development and Evaluation of IEEE 802.11 Intrusion Detection Systems (IDS)," November 2005.

enterprise networks. Their laptops and devices are normally outside DHS control.

Separate wireless network infrastructure is to be used for official visitors—either logically or physically separated from the DHS internal wireless or wired networks. The only purpose of the official visitor wireless network is to enable visitors to wirelessly access the Internet using visitor-owned devices.

A shared key encryption scheme, WPA2-Pre-Shared Key (PSK), offers a cost-effective way to limit WLAN traffic to authorized visitors. The PSK is shared by all visitors and may not protect traffic among visitors. The encryption key should be changed periodically, for example, weekly.

3.9 Perimeter Security

Perimeter security devices include firewalls, VPN concentrators, IDS/IPS, and so on. These devices provide access control, encryption and decryption for message confidentiality, and the detection of security policy violations.

3.10 Radio Coverage and Power Level

The RF signal strength and noise level need to be measured carefully at the coverage area to provide acceptable WLAN services. The leakage of wireless RF signals beyond the defined coverage areas should be minimized, which can be accomplished by fine-tuning the AP RF power and by positioning of the AP and its antenna.

The following elements should be considered for determining wireless coverage and service performance: signal strength, noise level, and SNR. Channel usage should be coordinated and designed with care to avoid overlap and interference.

4.0 FIXED ACCESS WIRELESS NETWORKS: SECURITY GUIDELINES

A fixed access wireless network is a network covering a wide geographical area, involving several point-to-point or point-to-multipoint nodes. Applications of this technology are employed when interconnecting two or more locations with RF line-of-sight (LOS) or near-LOS devices called bridges. Point-to-point connections typically involve the use of highly directional antennas that can be tuned to span great distances, as long as the area between the two points is free of obstructions. Point-to-multipoint configurations form a hub-and-spoke topology with a master bridge located in a central position and multiple client bridges. The master bridge typically employs an omni-directional antenna. One such technology is the point-to-point microwave connection that has been used widely for voice and data communications

Bridges are typically employed in a fixed-access wireless network to provide OSI Layer 2 connectivity between sites. It is important to secure bridged networks because beam scattering may allow unauthorized users to monitor network communications. Bridge links must be secured by encryption and access controls. Bridge devices must provide strong access controls, authentication, and configuration management. To provide defense in depth, additional network layer devices should be installed at site ingress and egress points.

- Bridge devices should be configured to accept connections only from other authorized and approved bridge devices and not from client devices.

4.1 BRIDGE LINK CONFIDENTIALITY

Bridges are a means of providing a mechanism to ensure that information is not made available or disclosed to unauthorized individuals, entities, or processes; to comply with DHS policy, select FIPS 140-2 validated products that use AES-256 encryption to secure link-level communications between bridges.

4.2 BRIDGE LINK AUTHENTICATION

One common practice is to deploy a MAC-address-based access control which only allows network connections for those devices if their MAC addresses are on a pre-defined MAC address list. MAC addresses within data frames are sent in the clear and, therefore, can be captured and eventually spoofed by attackers, but this security control prevents accidental connections and forces attackers to perform additional work to compromise the system.

4.3 BRIDGE RADIO COVERAGE RECOMMENDATIONS

The following elements should be considered for determining outdoor coverage and performance: antenna gain, antenna azimuth, antenna height, transmitter power, receiver sensitivity, cable losses, interference, and environmental structures.

5.0 WWAN: SECURITY GUIDELINES

A wireless wide area network (WWAN) is a network covering a wide geographical area, involving a vast array of clients. Wireless technology standards include Long Term Evolution (LTE), WiMAX, 802.11, and others. Commercial WWAN services such as cellular telephone service, packet radio networks, satellite communications, and WLAN hotspots provide a flexible and robust means for remote access and telework or extending DHS network coverage. However, these networks should be treated as untrusted public networks. DHS does not have control over the commercial service infrastructure, its configuration, operation, or maintenance, nor over the personnel with access to the infrastructure or management systems.

5.1 WWAN BUILT-IN SECURITY FEATURES

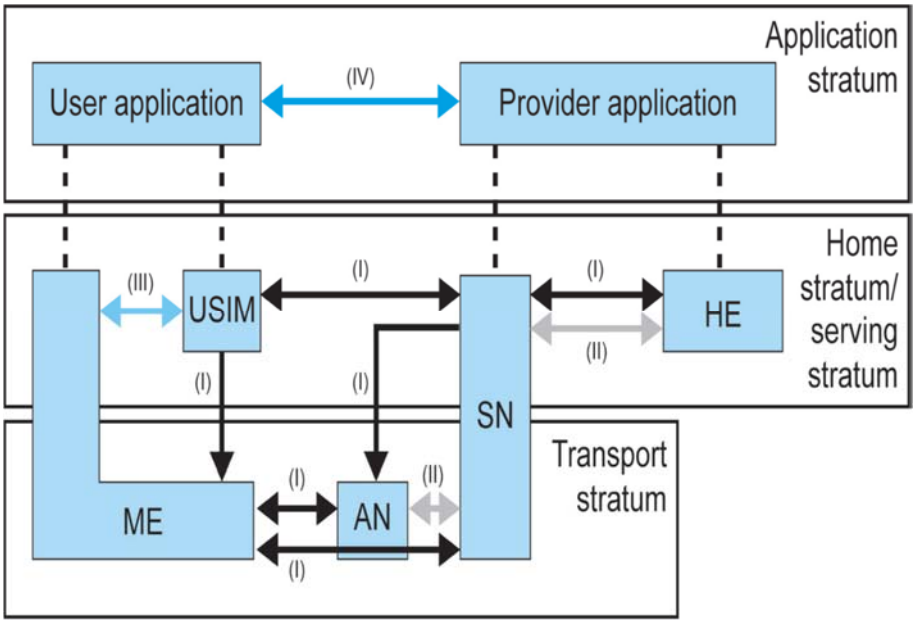
Different WWAN technologies implement various built-in security features based on the technology standards, and they are developed through the layered architecture approach. Security enhancement is implemented at all OSI layers, from lower physical medium all the way up to applications, as illustrated by the following common WWAN standards.

- The **IEEE 802.11i** standard implements the AES-Counter with Cipher Block Chaining (Counter with CBC)-Message Authentication Code (MAC) Protocol (AES-CCMP) to negotiate MAC-Layer specification security communications and establish the Layer 2 security connection that includes frame authentication, encryption, and integrity check. In addition, 802.1X port-based access control and EAP authentication, as well as the security measures at upper layers discussed in Section 3, are part of the overall security architecture.
- The **IEEE 802.16** standards define the air interface and Medium Access Control (MAC) for a Wireless Metropolitan Area Network (WMAN). This is the first industry-wide standard suite that can be used for fixed, nomadic, and mobile wireless access with substantially higher bandwidth than the cellular networks. The 802.16d (Fixed WiMAX) standard provides an alternative to cabled access networks, such as fiber optic, cable modem, and digital subscriber line (DSL). The 802.16e (Mobile WiMAX) standard provides mobile voice, video and Internet services similar to 3G cellular, but with a higher data rate. The IEEE 802.16 devices need to be certified by the WiMAX forum to ensure interoperability. The IEEE 802.16 standards provide user authentication and data privacy as security measures. Privacy key management (PKM) is used for user authentication. PKM establishes a security association between the base station and subscriber device. The security association is a set of security information that a base station and one or more subscribers share to support secure communications. PKM distributes an authorization token to an authorized subscriber by verifying the subscriber's digital certificate. AES with at least 128 bits is used to ensure data privacy.
- **Satellite** network security measures include, among other means, encryption, high-power uplinks, spread spectrum, and digital interface certifications.

Satellite networks generally employ proxy-based techniques to overcome the shortcomings associated with satellite communications: low bandwidth, long delay, and high error rate. Transmission Control Protocol (TCP) Performance Enhancing Proxy (PEP) is implemented to intercept TCP packets, break the connections, and act as a proxy server for both ends, all in an effort to improve TCP performance. Similar techniques are also used to improve the speed of responses to Web-browser requests and responses via HTTP proxy servers.

The proxy approach requires that part of communication messages, TCP header or Web page request and response, be in clear text and be available to proxy servers, which may be controlled by third parties. The proxy mechanism can be disabled, which leads to performance degradation. It is extremely important for organizations to understand the satellite proxy mechanism, evaluate the performance requirements, and make an informed and balanced decision from both operational and security perspectives.

- **LTE** has been chosen as a 3G/4G cellular technology by major cellular service providers around the globe. Specifically, the International Telecommunication Union (ITU) has approved LTE-Advanced as a candidate for 4G technologies. LTE and LTE-Advanced are standardized by the Third Generation Partnership Project (3GPP). LTE defines the security features at the application, device, and transport levels.[3] This security architecture is also applicable to 3G cellular networks.



AN	Access Network	HE	Home Environment
ME	Mobile Equipment	SN	Serving Network

[3] 3rd Generation Partnership Project, "3GPP System Architecture Evolution (SAE): Security architecture (Release 8)."

USIM	Universal Subscriber Identity Module		

Figure 1. LTE Security Architecture

Five security feature groups are defined, as shown in the figure above. Each of these feature groups meets certain threats and accomplishes certain security objectives:

- **Network access security (I) –** the set of security features that provides users with secure access to services, and which protects against attacks on the (radio) access link.
- **Network domain security (II) –** the set of security features that enables nodes to securely exchange signaling data and user data and protect against attacks on the wireline network.
- **User domain security (III) –** the set of security features that secures access to mobile stations.
- **Application domain security (IV) –** the set of security features that enables applications in the user and provider domains to securely exchange messages.
- **Visibility and configurability of security (V) –** the set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

Based on these specifications, some commercial LTE service providers implement the security features through Universal Integrated Circuit Card (UICC), Subscriber Identity Module (SIM), and key authentication using128-bit private keys. LTE also provides strong mutual authentication, user identity confidentiality, and integrity protection of signaling messages between end user devices and service provider networks.

Although the WWAN built-in security features sometimes do not offer the desired strong cryptographic capabilities (e.g., the AES key length is only 128-bit), they nevertheless provide one layer of defense against wireless security threats.

5.2 PRIVATE WWAN

Similar to the wired network private WAN concept, a new WWAN operation model has emerged through which commercial wireless service providers allow a certain group of customers to access their wireless networks anywhere but isolate the data traffic of this group from the rest as well as the Internet, effectively providing a dedicated and isolated private WWAN service.

A private WWAN enhances wireless communication security as the network is within the accreditation boundary established by DHS and over which DHS has direct control for the application of required security controls or the assessment of security control effectiveness. It

provides visibility of all traffic thereby enabling the identification of and protection against malicious activities.

5.3 REMOTE ACCESS THROUGH VPN SERVICE

When DHS users access DHS internal resources via commercial WWAN, they should follow standard remote access guidelines and procedures. Secure remote access can be achieved through DHS VPN services that offer strong encryption, authentication, and access control mechanisms to ensure information security for sensitive data transferred across multiple, public networks.

6.0 WIRELESS PERSONAL AREA NETWORKS: SECURITY GUIDELINES

A wireless personal area network (WPAN) is a network for interconnecting peripheral devices in a short range (up to the order of tens of meters). Two common technologies under the WPAN category are IEEE 802.15.1 (also known as Bluetooth) and IEEE 802.15.4 (also known as ZigBee). WPANs are typically established in an ad hoc or peer-to-peer fashion without any static infrastructure. The security capability associated with WPAN is not sufficient for protecting sensitive information. Operation of such noncompliant systems requires an approved waiver or exception, as appropriate, from the CISO.

6.1 AD HOC OR PEER-TO-PEER NETWORKS

WPAN client devices should not be allowed to create ad hoc or peer-to-peer networks. If the CISO approves the use of such networks, the system owner shall provide documentation detailing security policies, procedures, and technical security capabilities and limitations.

6.2 DEVICES

It is important that IT security managers identify the WPAN capabilities in all personally owned devices present in the organization in order to educate users about the risks inherent in these devices and to mitigate vulnerabilities through effective countermeasures. Users must ensure that WPAN capabilities on their devices (e.g., Bluetooth, IR, and RF ports) are disabled or rendered inoperable before their entry into sensitive environments to prevent sharing information with untrusted and/or unauthorized users.

6.3 COVERAGE AND POWER REQUIREMENTS

Device power requirements vary depending on the application being used. The RF power output level should be the minimum needed to support the particular wireless application in use. This limits the distance from which eavesdroppers can listen in and/or stage attacks.

6.4 BLUETOOTH DEVICE COMMUNICATION RISKS AND RECOMMENDATIONS

For Bluetooth communications, critical information is passed between devices during and after pairing, which, if captured, could allow an attacker to gain full remote access to the WPAN device. Several Bluetooth versions are currently available such as high-speed 3.0 and Low Energy (LE) 4.0, and they support different levels of security modes. For example, for Bluetooth 3.0, Security Mode 3 is the strongest mode because it requires establishment of authentication and encryption before the Bluetooth physical link is completely established. More information on Bluetooth security can be found in NIST SP 800-48, *Wireless Network Security 802.11, Bluetooth and Handheld Devices* (November 2002), and NIST SP 800-121, *Guide to Bluetooth Security* (June 2012).

6.5 PERSONAL IDENTIFICATION NUMBER PROTECTION

WPAN device communications typically rely on the device's hardware address for identification and a PIN for authentication. If possible, PINs should be generated randomly, avoid identifiable

patterns, and be sufficiently long to ensure that the PIN is not easily ascertained by unauthorized users. For example, Bluetooth security is only as strong as the PIN the user selects and will typically range between 4 and 16 bytes.

Devices that are not configurable typically have a hard-coded manufacturer PIN that creates a vulnerability that an attacker can exploit. For example, attackers can determine a hard-coded PIN by reading the device's user manual or by inspecting the device while left unattended. These devices also do not allow the user to disable discovery mode. While eavesdropping on a Bluetooth mouse would only provide an attacker with X and Y coordinates, eavesdropping with an ear-bud microphone would allow the attacker to intercept a complete telephone conversation.

6.6 Disabling Unwanted Profiles

One example of a profile for Bluetooth WPANs that could potentially expose sensitive information is the Object Exchange Protocol (OBEX). This profile, if exploited, could provide an attacker with unrestricted file access and file push capabilities. Theft of information from a wireless device through a Bluetooth connection is commonly known as bluesnarfing.

6.7 Device Security Capabilities

WPAN-enabled devices provide various security capabilities in the areas of encryption, authentication, and data integrity. The strongest security modes should be chosen to provide an extra layer of security, even though they often do not meet the DHS security standards (e.g., the encryption key is shorter).

7.0 INTEROPERABILITY

Organizations operating across many physical locations, mission groups, agencies, and commercial networks may require a wireless infrastructure that allows for interoperable mobile computing with diversified platforms and wireless standards. Standards, protocols, and products approved for use within DHS can be found in the DHS Technical Reference Manual (TRM) documents. However, devices that are listed in the TRM and follow IEEE or NIST standards may still be subject to interoperability challenges. This section will address wireless system interoperability concerns and recommendations.

7.1 INTEROPERABILITY GOVERNING BODY

Even following the same IEEE or NIST standards, wireless equipment and respective security implementations for a given wireless network may have different configurations from those of other networks of interest and may require additional means for interoperability. For example, within WLAN networks based on the same IEEE 802.11 standard, AP from different vendors typically cannot communicate among themselves, as some of them are thin AP (basically a pass-through device) while others are thick AP (performing, among other functionalities, authentication and encryption). Consequently, a dedicated DHS organization, such as the TRM governing body, should coordinate the activities of specifying, designing, and establishing wireless systems for purposes of interoperability. The TRM governing body can be the central coordinator for resolution of cross-organizational interoperability issues and may need to perform research and coordinate with other wireless-enabled Components or agencies during the system design process.

7.2 WIRELESS SYSTEM INTEROPERABILITY

As wireless networks increase in density, enterprise applications that use wireless connections can be expected to gain in popularity. Many emerging technologies take advantage of multiple APs or even multiple distinct wireless networks; examples are Wireless Voice over IP (W-VoIP) and location-based services that leverage beacons from wireless networks to provide location services. These technologies maintain connections to one or more internally or externally wireless networks in a mobile fashion, otherwise known as roaming. The challenge is to provide seamless wireless services across different technologies or organization domains.

Although APs communicate with user devices via standard wireless protocols such as IEEE 802.11 a/b/g/n, the communication mechanisms between APs and wireless backend systems such as wireless controllers are almost all proprietary. Therefore, it is almost impossible for an AP from Vendor A to communicate with another AP or controller from Vendor B.

One way to address these issues is the adoption of Mobile IP mechanism (or IP mobility), which is an Internet Engineering Task Force (IETF) standard communications protocol that supports mobile device users to move from one wireless network to another by assigning two IP

addresses to a mobile device. One address is the static permanent home address. The second address, the "care-of" address, is the dynamic address assigned by the current wireless network. All application packets are sent to the home IP address and the home wireless network forwards the packets to the current IP address (and therefore the mobile device).

7.3 WIRELESS STANDARDS

Wireless architectures ideal for interoperable communications among coordinating organizations should incorporate products designed with wireless communications standards. Wireless products built upon proprietary standards should be avoided.

As discussed in Section 3.1, new security standard 802.11w, which was added to WPA2 in 2012, addresses the protection of management frames. However, support of the 802.11w standard among wireless devices is very limited.

Other standards have also been developed to address interoperability of different wireless standards in order to provide seamless wireless services. IEEE 802.21is one interoperability standard for communication among IEEE 802 and non-802 networks, such as 802.3, 802.11, 802.15, 802.16, and cellular networks. The Unlicensed Mobile Access (UMA) technology alliance is developing interoperability specifications for communications roaming across cellular, WLAN, and Bluetooth systems. The enforcement of standards and industry certifications increases the probability of multiple organizations' systems working together with minimal user intervention.

APPENDIX A – ACRONYMS

Acronym	Definition
3GPP	Third Generation Partnership Project
AD	(Microsoft) Active Delivery
AES	Advanced Encryption Standard
AO	Authorizing Official
AP	Access Point
ARP	Address Resolution Protocol
C&A	Certification and Accreditation
CBC	Cipher Block Chaining
CCMP	Cipher Block Chaining (Counter with CBC)-Message Authentication Code (MAC) Protocol
CDP	Cisco Discovery Packet
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DAA	Designated Accrediting Authority
dB	Decibel
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DoD	Department of Defense
DoS	Denial of Service
DSL	Digital Subscriber Line
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
ESSID	Extended Service Set Identifier
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act

Acronym	Definition
GAO	Government Accountability Office
HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
IDS	Intrusion Detection System
IEEE	Institute for Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IR	Infrared
IT	Information Technology
ITU	International Telecommunication Union
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LOS	Line of Sight
LTE	Long Term Evolution
MAC	Media Access Control
Mbps	Megabits per second
NAC	Network Access Control
NCPS	National Cyber Protection System
NDS	Novell Directory Service
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVD	National Vulnerability Database

Acronym	Definition
OBEX	Object Exchange Protocol
OCISO	Office of the Chief Information Security Officer
OSI	Open Systems Interconnection
PD	Policy Directive
PEAP	Protected Extensible Authentication Protocol
PEP	Performance Enhancement Proxy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKM	Privacy Key Management
PP	Protection Profiles
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
ROB	Rules of Behavior
SAP	Security Authorization Package
SIM	Subscriber Identity Module
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise
SOP	Standard Operating Procedure
SSH-2	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TCP	Transport Control Protocol
TCP/IP	Transport Control Protocol/Internet Protocol
TIC	Trusted Internet Connections
TKIP	Temporal Key Integrity Protocol

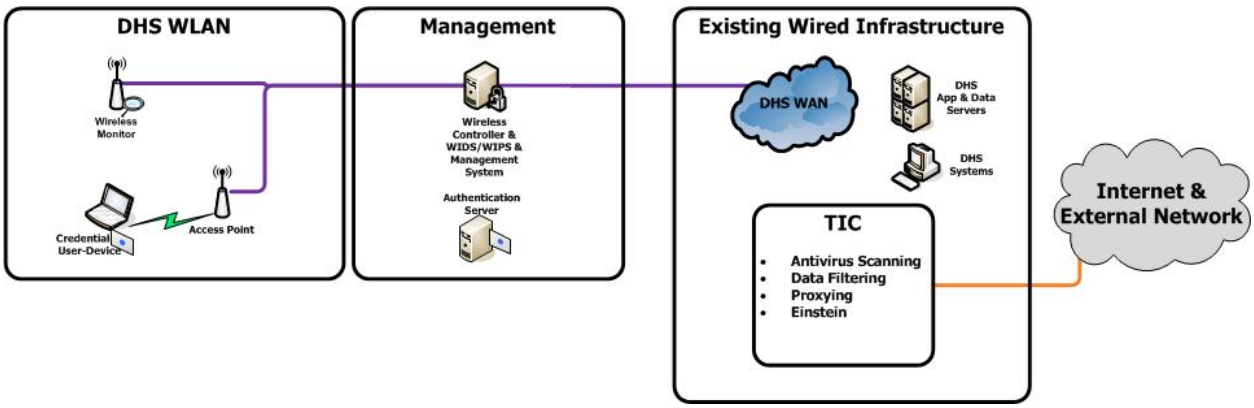
Acronym	Definition
TRM	Technical Reference Manual
UICC	Universal Integrated Circuit Card
UMA	Unlicensed Mobile Access
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPA2	Wireless Protected Access 2
WPAN	Wireless Personal Area Networks
WPS	Wireless Protected Setup
WWAN	Wireless Wide Area Networks
W-VoIP	Wireless Voice over Internet Protocol

APPENDIX B – WLAN SYSTEM ARCHITECTURE

This appendix describes the key components of WLAN infrastructure and their functionalities and provides high-level WLAN system architecture diagrams. The diagrams provide a depiction of generic WLAN systems in order to highlight the basic components of a WLAN and how it relates to the enterprise-wide network infrastructure.

Table B-1. Key Components of WLAN Infrastructure

Component	Provides:
User-Device	• WPA2-Enterprise encryption • Device authentication using EAP • Device certificate • User authentication
Access Point	• Wireless connection
RADIUS Authentication Server	• Authentication services
WIDS/IPS	• Rogue AP detection • Unauthorized client detection • Unauthorized access attempts • Continuous monitoring of 802.11 channels • Monitoring for user devices connected to both wireless and wired networks
Wireless Controller	• Centralized management of wireless APs and user Devices • Monitoring, control, and configuration of APs; enforcement of security policy
Management System	• Centralized management and configuration software



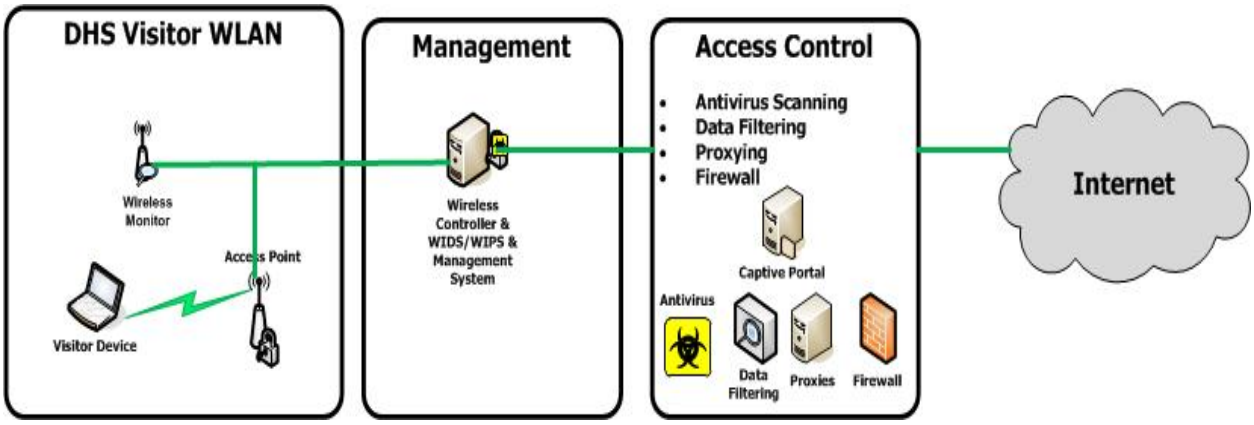


Diagram B-1. Notional WLAN Architecture Diagrams: Internal WLAN (top) and Visitor WLAN (bottom)

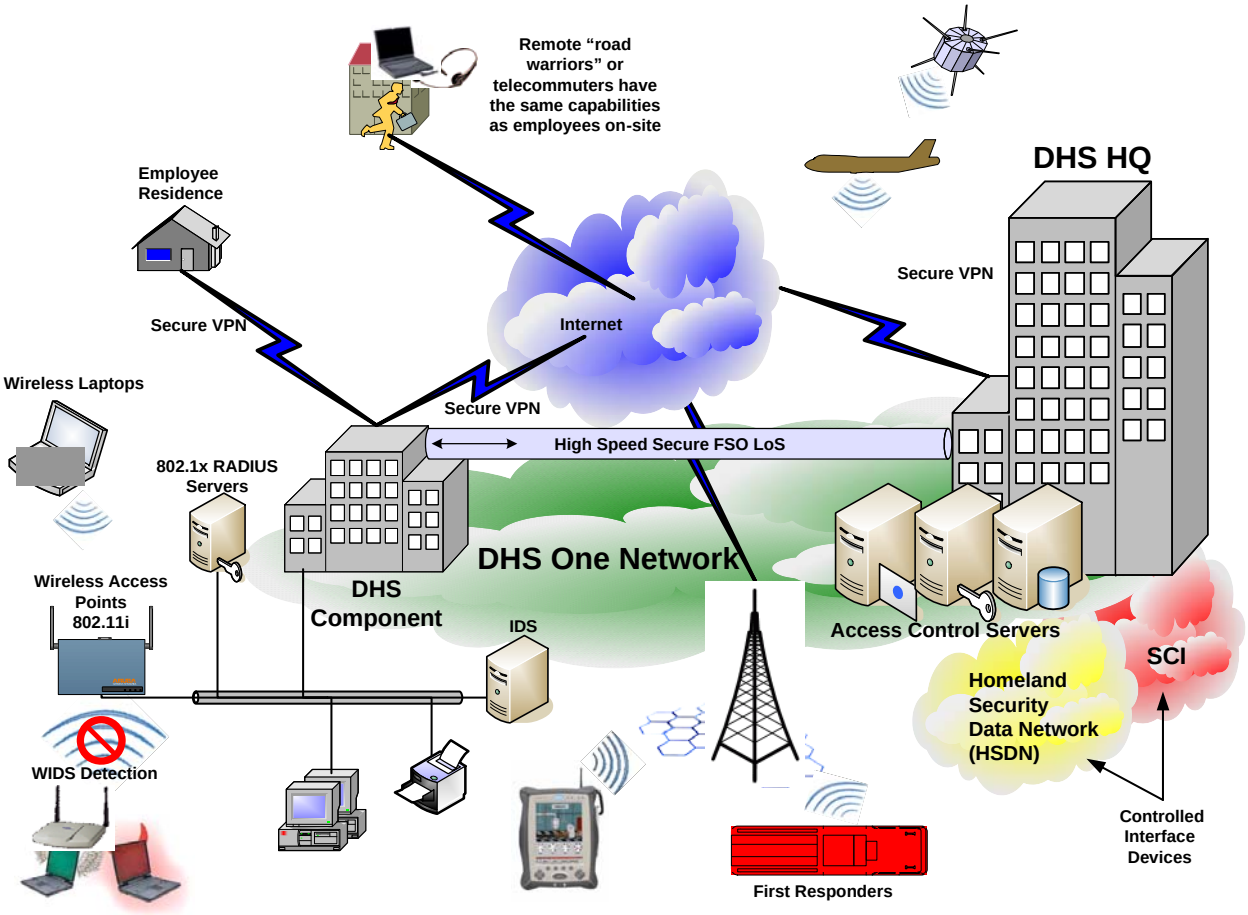


Diagram B-2. Notional DHS Enterprise Architecture

APPENDIX C – SECURITY REQUIREMENTS CHECKLIST FOR MOBILE SYSTEMS

Mobile Feature and Configuration Guidance			
SECTION 2.0 REQUIREMENTS FOR ALL WIRELESS SYSTEMS			
☐	**Section 2.1: Risk-Based Approach**	**Required**	**Recom-mended**
	A risk-based approach shall be used to mitigate risks associated with wireless systems.	X	
☐	**Section 2.2: Wireless System Threats and Countermeasures**	**Required**	**Recom-mended**
	Sensitive wireless systems shall have the capability to detect, locate, and identify attacks, as well as to capture transmissions for forensic analysis.	X	
	Security guidelines for layers of the Open Systems Interconnection (OSI) model are followed when designing and implementing wireless systems.		X
☐	**Section 2.3: Authentication**	**Required**	**Recom-mended**
	Wireless systems shall employ IEEE 802.1X port-based authentication methods.	X	
	Every system administrative password shall be changed to a strong password that complies with overarching organization password conventions defined in DHS 4300A.	X	
	Systems should not operate using default factory passwords; these must be changed prior to the system being put into operational use.		X

Mobile Feature and Configuration Guidance			
⍰	**Section 2.4: Confidentiality**	**Required**	**Recom-mended**
	Wireless systems shall use the FIPS 140-2 validated AES-256 encryption to protect the confidentiality of data.	X	
	The use of static keys should be avoided.		X
	Dynamic key rotation should be used in conjunction with an enterprise RADIUS server.		X
	End-to-end encryption shall be implemented across wireless and wired networks to protect the confidentiality of data.		X
⍰	**Section 2.5: Integrity**	**Required**	**Recom-mended**
	FIPS 140-2 validated hash routines and security controls should be used to ensure data have not been modified in an unauthorized or accidental manner.		X
	Protocol built-in integrity capabilities should be enabled to ensure data integrity.		X
⍰	**Section 2.6: Management Control**	**Required**	**Recom-mended**
	A centralized wireless management control structure shall be used that is integrated with the existing wired network.	X	
⍰	**Section 2.7: Physical Security**	**Required**	**Recom-mended**
	Each wireless infrastructure device should be installed in a secured enclosure or space that is resistant to tampering, theft, and unauthorized access to console ports, power supplies, and reset buttons.		X
	Guards who routinely patrol the facilities should visually inspect AP enclosures.		X

Mobile Feature and Configuration Guidance			
	Guards should be made aware of the importance of these devices and the likelihood of potential theft or tampering, as well as be able to recognize signs of tampering or unauthorized individuals attempting to access the enclosures.		X
⍰	**Section 2.8: National Information Assurance Partnership Common Criteria Security Validations**	**Required**	**Recom-mended**
	DHS administrators should carefully evaluate products to ensure that security validations have been performed and that the products conform to commonly used PPs.		X
	The NIAP validation reports should be examined carefully to ensure that all required targets of evaluation are validated to an appropriate level of robustness.		X
	Protocols that send clear text passwords, or otherwise do not use a secure protocol such as Telnet, HyperText Transport Protocol (HTTP), Simple Network Management Prot0ocol (SNMP) v1/2, and Cisco Discovery Protocol (CDP), are not used as a means of in-band device management that are enabled by default and are not essential to mission requirements should be disabled.		X
	Ports, protocols, and services that are enabled by default and are not essential to mission requirements should be disabled.		
	Processes that send clear text passwords or otherwise do not use a secure protocol (e.g., Telnet, HyperText Transport Protocol [HTTP], Simple Network Management Protocol [SNMP] v1/2, or Cisco Discovery Protocol [CDP]), should not be used as a means of in-band device management.		X
	Wireless systems should be tested and inventoried regularly (e.g., quarterly) for compliance with the organization's list of approved ports and protocols.		

Mobile Feature and Configuration Guidance			
⍰	**Section 2.9: Logs**	**Required**	**Recom-mended**
	Systems should be configured to create logs and capture important events such as successful and unsuccessful administrator logins, client device access attempts, client device MAC addresses, access violations, associations, disassociations, ports and protocols used, and user activities.		X
	Log entries should be captured by a remote system on the wired network to make the organization's overall network less vulnerable to attack.		X
	Log management should be addressed in the organization's Security Plan for that system.		X
⍰	**Section 2.10: Configuration Control**	**Required**	**Recom-mended**
	Configuration requirements shall be established for wireless networks and devices in accordance with the developed security policies and requirements.	X	
	All sensitive settings for wireless systems should be changed from vendor defaults to protect against unauthorized intrusion and modification of system settings.	X	
⍰	**Section 2.11: Software and Firmware Updates**	**Required**	**Recom-mended**
	Security updates and patches should be applied to all system devices to ensure that up-to-date firmware and software that protects these systems against known vulnerabilities are installed.		X

Mobile Feature and Configuration Guidance			
⍰	**Section 2.12: Wireless Monitoring**	**Required**	**Recom-mended**
	The RF signal should be constantly monitored to ensure minimal signal leakage.		X
	WIDP/IPS shall monitor the wireless infrastructure to detect suspicious activities.	X	
⍰	**Section 2.14: Traffic Separation**	**Required**	**Recom-mended**
	Traffic from different security trust boundaries shall be logically and/or physically separated.	X	
⍰	**Section 2.15: Security Assessment**	**Required**	**Recom-mended**
	Regular (at least annual) security assessment shall be performed to assess the wireless system security capabilities and discover any potential vulnerability.	X	
⍰	**Section 2.16: Security Incident Response**	**Required**	**Recom-mended**
	The security incident response standard operating procedures (SOP) shall specify methods for wireless system users and other personnel to report security incidents in accordance with DHS 4300A.	X	
	Section 2.17: Security Awareness Training	**Required**	**Recom-mended**

Mobile Feature and Configuration Guidance			
	In accordance with DHS Sensitive Systems Policy Directive 4300A, Components provide annual wireless security awareness training. The security awareness training may be combined with similar training for other systems and may be provided during an employee's orientation program.		
	Technical training of personnel shall include hands-on instruction on how to operate the wireless systems or devices assigned to them within the context of their roles and responsibilities.		
	All employees who use or administer the wireless system shall complete security awareness training prior to use of the system.		
	Evidence of completion submitted to the Information System Security Manager (ISSM) of the program or the appropriate security authority.		
	Components should create Rules of Behavior (ROB) agreements that specifically cover policies and procedures for wireless systems.		
	Users are required to receive a Rules of Behavior document whenever rights to access wireless systems are first granted and again during annual inventory re-certifications.		
	Component policies and procedures for wireless systems should ensure that Policies and procedures should ensure that all users sign and return a Rules of Behavior document when their wireless system access is first issued.	X	
Section 3.0: WLAN Security Guideline			
⍰	**Section 3.1: Security Approach**	**Required**	**Recom-mended**
	WLAN systems shall meet the Wi-Fi Alliance Wireless Protected Access 2 (WPA2) interoperability standard that is based on the Institute for Electrical and Electronics Engineers (IEEE) 802.11i security standard.	X	

Mobile Feature and Configuration Guidance			
	WLAN systems shall use the IEEE 802.11w security standard if such standard is supported by the systems	X	
⍰	**Section 3.2: WLAN Network Naming Conventions**	**Required**	**Recom-mended**
	The WLAN network name should be changed from the default name to a unique name that does not reveal DHS sensitive information.		X
⍰	**Section 3.3: ESSID Broadcasting**	**Required**	**Recom-mended**
	The wireless automatic connection capability should be disabled.		X
	DHS wireless users should not connect to any unknown wireless networks.		X
⍰	**Section 3.4: Access Control**	**Required**	**Recom-mended**
	Two-factor authentication (username/password, public key infrastructure [PKI] certificate, biometrics, or one-time-password, etc.) should be implemented as an access control mechanism for authorizing system access to WLANs.		X
	WLAN systems should implement 802.1X or equivalent network access control solutions as well as or in conjunction with EAP-TLS mutual authentication.		X
	The NAC system should have the ability to identify users and their devices and apply access control accordingly.		X

Mobile Feature and Configuration Guidance			
⍰	**Section 3.5: Encryption**	**Required**	**Recom-mended**
	Static WEP encryption offered by 802.11-based networks should NOT be used.		X
	WLAN systems shall implement a NIST FIPS-approved mode with AES-256 encryption.	X	
	Systems that provide per-session dynamic RC4 keys, such as dynamic WEP, temporal key integrity protocol (TKIP), and WPA, are not FIPS 140-2 approved and thus shall NOT be adopted.		X
⍰	**Section 3.6: WIDS**	**Required**	**Recom-mended**
	WIDS has these capabilities: • Performs direction finding/triangulation to locate unauthorized AP or other wireless devices • Tracks the connection status of all clients • Detects bridging connections from wireless to the wired network directly in a wireless end-user device • Detects any RF interference sources with physical location information	X	
⍰	**Section 3.7: WIPS**	**Required**	**Recom-mended**
	WIPS blocks or removes wireless end-user devices that have been determined to be a threat on the WLAN.	X	
⍰	**Section 3.8: Official Visitor Network**	**Required**	**Recom-mended**
	A separate wireless network infrastructure is used for official visitors—either logically or physically separated from the DHS internal wireless or wired networks.	X	

Mobile Feature and Configuration Guidance			
	Official visitors accepts pre-defined DHS wireless use terms and conditions prior to accessing the visitor network. Content filtering, monitoring, logging, and other security measures should be deployed for the visitor network.	X	
	Records are maintained to demonstrate that all official accept pre-defined DHS wireless use terms and conditions prior to accessing the visitor network.	X	
	Content filtering, monitoring, logging, and other security measures are deployed for the visitor network.		X
⍰	**Section 3.9: Perimeter Security**	**Required**	**Recom-mended**
	The interconnection point between the wired and the wireless network should be segmented with perimeter security devices to ensure that all devices operating on the WLAN comply with the DHS IT Security Policy.		X
⍰	**Section 3.10: Radio Coverage and Power Control**	**Required**	**Recom-mended**
	RF footprint and power output are adjusted to minimize RF leakage; for instance, a signal-to-noise ratio (SNR) of 25 decibels (dB) for data service (allowing a data rate of about 10 megabits per second [Mbps]) and 35 dB or more for Voice over Internet Protocol (VoIP) are two common parameters for acceptable wireless services.		X
SECTION 4: FIXED ACCESS WIRELESS NETWORKS			
⍰	**Section 4.0: Bridge Configuration**	**Required**	**Recom-mended**

Mobile Feature and Configuration Guidance			
	Bridge devices should be configured to accept connections only from other bridge devices and not from client devices.		X
⍰	**Section 4.1: Bridge Link Confidentiality**	**Required**	**Recom-mended**
	FIPS 140-2 validated products using AES-256 are used to secure link-level communications between bridges.	X	
⍰	**Section 4.2: Bridge Link Authentication**	**Required**	**Recom-mended**
	Bridges provide a mechanism to mutually authenticate each other before communications are established and periodically during the communications.		X
	Bridges provide a mechanism to ensure data integrity.		X
	MAC-address-based access control capabilities are configured on all bridges so that any connection from any other bridge that is not specifically allowed will be denied by default.		X
⍰	**Section 4.3: Bridge Ratio Coverage Recommendations**		**Recom-mended**
	Bridge RF footprint and power output are adjusted to minimize RF leakage		X
SECTION 5.0: WWAN			
⍰	**Section 5.1: WWAN Built-in Security Features**	**Required**	**Recom-mended**
	WWAN built-in security features are enabled.		X

Mobile Feature and Configuration Guidance			
⍰	**Section 5.2: Private WWAN**	**Required**	**Recom-mended**
	DHS encryption, authentication, and security control standards are applied to the private WWAN.	X	
⍰	**Section 5.3: Remote Access Through VPN Service**	**Required**	**Recom-mended**
	DHS remote access security guidelines and procedures are followed when users access DHS internal resources via commercial WWAN.	X	
SECTION 6.0: WIRELESS PERSONAL AREA NETWORKS: SECURITY			
⍰	**Section 6.1: Ad Hoc and Peer-to-Peer Networks**	**Required**	**Recom-mended**
	Strict configuration restriction of ad hoc and peer-to-peer networks on client devices are enforced.		X
	Ad Hoc and peer-to-peer networks are disabled immediately when they are no longer necessary.		X
	A regular (e.g., weekly) scan and audit are performed to ensure that unauthorized Ad Hoc and peer-to-peer networks are identified and disabled.		X
	Section 6.2: Devices	**Required**	**Recom-mended**
	Any WPAN capabilities that are not required by users are deleted or disabled.		X

Mobile Feature and Configuration Guidance			
	Security personnel are properly trained to recognize PAN-capable devices and be familiar with disabling PAN functions in those devices.		X
	Weekly scan and audit for these devices are being performed to ensure the proper enforcement of DHS policies and procedures.		X
?	**Section 6.3: Coverage and Power Requirements**	**Required**	**Recom-mended**
	The RF footprint and power output of devices are adjusted to minimize RF leakage.		X
?	**Section 6.4: Bluetooth Device Communication Risks and Recommendations**	**Required**	**Recom-mended**
	IT security managers ensure that Bluetooth communications are conducted in an environment where information exchanged cannot be captured by eavesdroppers.		X
	Communication are restricted to private areas where there is limited RF signal propagation.		X
	To prevent devices from advertising themselves to would-be attackers, devices are configured for the non-discoverable mode unless the user is in the process of pairing Bluetooth devices.		X
	To avoid increased risks of vulnerable points of entry, multiple or split communications paths are not allowed for the same client device.		X
	The strongest security mode is used for Bluetooth communications. Details can be found in the NIST SP 800-121 for various Bluetooth versions.	X	

Mobile Feature and Configuration Guidance			
⍰	**Section 6.5: Personal Identification Number Protection**	**Required**	**Recom-mended**
	IT security managers avoid deploying or permitting the use of wireless devices that do not provide the necessary user interface to allow PINs to be changed or reconfigured (e.g., Bluetooth mice, ear-bud microphones, keyboards).		X
⍰	**Section 6.6: Disabling Unwanted Profiles**	**Required**	**Recom-mended**
	Unnecessary WPAN profiles are disabled to reduce the points of access an attacker might exploit.		X
	Organizations operate under the principle of least privilege and only enable functionality that users absolutely require for day-to-day operations.		X
SECTION 7.0: INTEROPERABILITY			
⍰	**Section 7.3: Wireless Standards**	**Required**	**Recom-mended**
	Only IEEE 802.11 a/b/g/n standards are used for wireless device data communication.	X	
	Only Wi-Fi Alliance WPA2 Enterprise certified devices are deployed, which is based on IEEE 802.11i standard.	X	
	Only IEEE 802.1X standards-based WLAN identification and authentication methods are used.	X	
	WLAN systems use the IEEE 802.11w security standard if such standard is supported by the systems.	X	

APPENDIX D – WIRELESS SYSTEM RULES OF BEHAVIOR USER AGREEMENT

The following rules describe when and how to use your access to wireless systems.

- Use **Government**-owned wireless systems only for authorized and official Government functions and such private functions as are specifically authorized by regulation.
- Use only **Government**-owned wireless systems to access **sensitive** information or connect to **DHS** systems.
- Comply with all copyright and licensing requirements associated with the use of wireless systems.
- Use personal firewalls, anti-virus software, and other protective mechanisms as required by DHS security policy and procedures. Update the virus protection software and its virus signature files at least weekly.
- Ensure that unauthorized persons cannot view the screen if it contains sensitive information.
- Remove all personal and sensitive information when returning a wireless device to government custody.
- Do not share or loan account passwords or permission to access **Government**-issued wireless devices.
- Do not load or run unauthorized software on wireless systems or wireless devices.
- Do not make any changes to the wireless system configuration unless directed to do so by an authorized System Administrator.
- Do not program wireless systems with sign-on sequences, passwords, or access telephone numbers.
- Do not leave a wireless device unattended, especially while it is unlocked/logged in. Follow published locking and log-off procedures.
- Do not use wireless systems in areas where classified information is processed or discussed.
- Do not use wireless systems containing audio, video, or photographic recording and/or transmission capabilities in areas where classified information is processed or discussed.

Wireless Device Protection

- Assume responsibility for taking all necessary precautions to protect wireless systems and data against loss, theft, damage, abuse, or unauthorized use by employing lockable cases and keyboards, locking cables, and removable media drives.
- Keep the wireless device under physical control at all times, or secure it in a suitable locked container under your control.

Identification and Authentication (I & A)

The following rules address passwords on wireless systems:

- Follow DHS policy on password management.
- Protect passwords from disclosure.
- Ensure that no one can observe the entry of passwords.
- Promptly change a password whenever compromise of that password is known or suspected.
- Do not attempt to bypass I&A measures implemented at the device and network levels.
- Do not store passwords, access numbers, or smart cards with the wireless system.
- Do not record passwords on paper or in electronic form or store them with or on the wireless system.

Data Protection

- Protect sensitive information from disclosure to unauthorized persons or groups.
- Use only Government Furnished Equipment to access sensitive DHS information, unless the AO has previously provided written authorization.
- Do not access, process, or store classified information on wireless systems without proper authorization.

Encryption and Public Key Infrastructure (PKI)

- Comply with DHS encryption and PKI requirements.
- Transmit data using wireless systems that rely on wireless encryption protocol (WEP) and/or use commercial wireless network providers only if the data is encrypted end-to-end using AES-256 VPN encryption.

- Do not shut down, disable, or reconfigure the encryption software or alter file permissions or policy settings in any way that might affect the encryption software or its proper operation.

Network Connectivity

- Use only Government-issued wireless devices to access sensitive DHS information or connect to DHS systems.
- Follow DHS policy on connecting computers and wireless systems to networks, including the Internet.
- Use only DHS-authorized Internet connections that conform to DHS security and communications standards.

Incident Reporting

- Immediately report confirmed or suspected security issues (e.g., operational anomalies, security violations, a missing or stolen wireless device, compromise of the encryption software) via established procedures for reporting security issues.

Traveling with a wireless device

- Back up all files before traveling.
- Keep the wireless device under your physical control at all times when traveling.
- Never place the wireless device in checked luggage.
- Never store the wireless device in an airport, train station, bus station, or any public locker.
- If leaving the wireless device in a car, lock it in the trunk out of sight.
- Avoid leaving the wireless device in a hotel room. If necessary, lock it inside another piece of luggage.
- Be prepared for airport security checks. Have the wireless device's batteries charged or a power cord handy so you can demonstrate that it is functional.
- Heighten vigilance at any security or luggage-scanning checkpoint. Place your wireless device on the conveyer belt only after the belongings of person ahead of you have cleared the scanner. If you are delayed, keep your eye on the wireless device.
- Exercise diligence when traveling in foreign countries because criminals or local intelligence may target your wireless device for the information it contains.

- Do not display any sensitive information on the wireless device screen when in any public place, such as an airport terminal, train or bus station, airplane, train, bus, or taxi.

Working From Home or an Alternate Workplace

- Implement security standards for hardware, software, and information to be used at the alternate workplace that are equivalent to those at the primary workplace.
- Provide physical security to protect the wireless system when not in use.

Consent Statement

I, _____, have read and understand the Rules of Behavior that apply to laptop computers and portable electronic devices. I agree to abide by these rules. I understand that failure to abide by these rules may result in disciplinary action.

I understand that DHS reviews telecommunications logs, computer logs, and telephone records and that it conducts spot-checks to determine compliance with controls placed on DHS IT resources.

I understand that I may acquire and use Sensitive information only in accordance with established policies and procedures. This includes properly destroying Sensitive information contained in hardcopy or softcopy and ensuring that Sensitive information is accurate, timely, complete, and relevant for the purpose for which it is collected, provided, and used.

I understand that any questions I may have regarding the security of wireless systems and data will be directed to my supporting Information Systems Security Officer (ISSO).

I acknowledge receipt of and understand my responsibilities for the use of DHS resources and will comply with the Rules of Behavior.

_____

Printed Name Organization

_____

Signature Date

Return this signed statement to _____ and retain a copy for your personal records.

U.S. CUSTOMS AND BORDER PROTECTION

ATTACHMENT Q4

SENSITIVE RFID SYSTEMS

HB 1400-05D

INFORMATION SYSTEMS SECURITY POLICIES AND PROCEDURES HANDBOOK

VERSION
7.0

NOVEMBER 16, 2017

This page intentionally blank

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
3.0	February 8, 2012	No changes.
4.0	May 10, 2013	No changes.
5.0	June 17, 2014	No changes.
5.1	October 30, 2014	Thorough rewrite. Major change to reflect new RFID technology development.
6.0	March 3, 2016	No Changes.
6.01	May 17, 2016	No Changes.
6.02	September 2016	No Changes.
7.0	November 16, 2017	No Changes.

CONTENTS

1.0 INTRODUCTION 1
1.1 Purpose 1
1.2 Scope 1
1.3 Authority 1
2.0 GOVERNANCE 2
2.1 RFID Usage Policy 2
2.2 Agreements with External Organizations 2
2.3 Privacy 2
2.4 Future Developments 3
3.0 STANDARD OPERATING PROCEDURES 3
3.1 Physical Access Control 3
3.2 Appropriate Placement of RFID Equipment 4
3.3 Secure Disposal of Tags 4
3.4 Separation of Duties 4
3.5 Configuration Management 5
3.6 Security Incident Response 5
3.6.1 Radio Frequency Interference 5
3.7 Continuity of Operations Planning 5
3.8 Security Auditing 5
3.9 Future Developments 6
4.0 RFID TECHNOLOGY SECURITY GUIDELINES 6
4.1 RFID Technologies 6
4.2 Active Tag Security 7
4.3 Passive Tag Security 8
4.4 Smart Card Security 9
4.5 Near Field Communication Security 9
4.6 Back-end System Security 10
4.7 Tag Data Security 10
4.8 RF Leakage 10
5.0 TRAINING AND EXERCISES 11
5.1 Security Awareness Training 11
5.2 Technical Training 11
APPENDIX A: REFERENCES 12
APPENDIX B: CHECKLIST FOR SECURING RFID SYSTEMS 13
APPENDIX C: PHYSICAL AND ENVIRONMENTAL SECURITY 23
APPENDIX D: ACRONYMS 24

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 GOVERNANCE STRUCTURES INVOLVING ORGANIZATIONS OUTSIDE DHS TO SUPPORT INTEROPERABILITY OF COMMUNICATION BETWEEN DHS COMPONENTS AND SUCH EXTERNAL ENTITIESSTANDARD 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.

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.

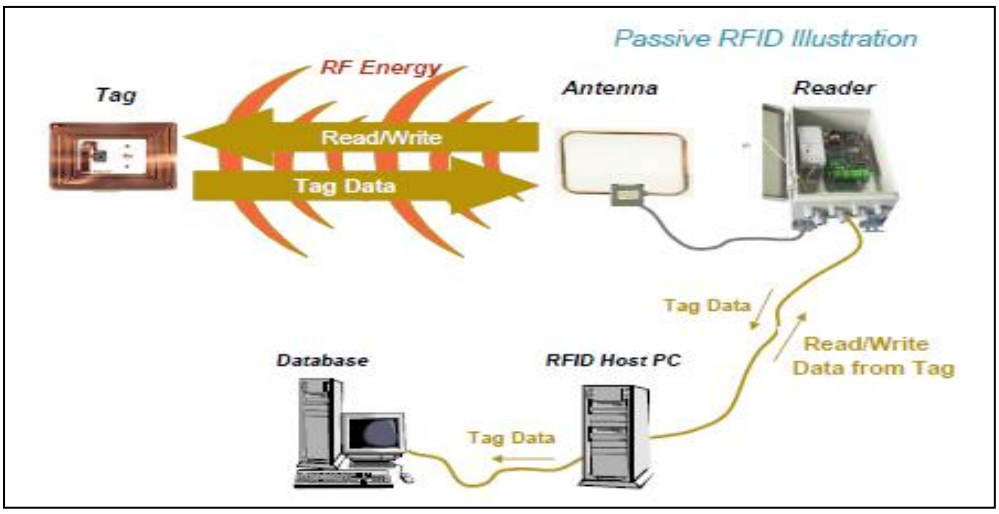


Figure 1: An RFID system and data flow.

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**	**Recommended**
	Any Component using RFID technology specifically documents and ensures that the use and users of RFID comply with DHS Sensitive Systems Policy Directive 4300A and all other related DHS RFID security and privacy policies.	X	
☐	**Section 2.2: Agreements With External Organizations**	**Required**	**Recommended**
	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**	**Recommended**
	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		X

	intended area of operation		
?	**SECTION 3.0: STANDARD OPERATING PROCEDURES**	**Required**	**Recommended**
	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**	**Recommended**
	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	X	

	boundaries.		
	Components use RF shielding on the perimeter of the RFID system implementation.		X
⍰	**Section 3.2: Appropriate Placement of RFID Equipment**	**Required**	**Recommended**
	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**	**Recommended**
	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**	**Recommended**
	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	Recommended
	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	X	

	submission of an emergency CR for retroactive approval of each emergency change. .		
	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	X	

	zeroization or degaussing for RFID system components, and destruction or using a KILL command for RFID tags.		
	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**	**Recommended**
	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**	**Recommended**
	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		X

	paper-based systems.		
	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**	**Recommended**
	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**	**Recommended**
	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**	**Recommended**
	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**	**Recommended**
	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**	**Recommended**
	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**	**Recommended**
	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**	**Recommended**
	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**	**Recommended**
	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

U.S. CUSTOMS AND BORDER PROTECTION

ATTACHMENT Q5

VOICE OVER INTERNET PROTOCOL (VOIP)

HB 1400-05D

INFORMATION SYSTEMS SECURITY POLICIES AND PROCEDURES HANDBOOK

VERSION
7.0

NOVEMBER 16 , 2017

This page intentionally blank

Document Change History

Version	Date	Description
6.0	Marh 3, 2016	New document.
6.01	May 17, 2016	No Changes.
6.02	September 2016	No Changes.
7.0	November 16, 2017	No Changes.

CONTENTS

1.0 INTRODUCTION **5**

1.1 Purpose and Scope *5*

1.2 VoIP Security Requirements Checklist *5*

2.0 VoIP System Overview **5**

2.1 VoIP System Architecture *5*

2.2 Federal Guidance and Polices *6*

3.0 THREAT OVERVIEW **7**

3.1 VoIP Threats and Vulnerabilities *7*

3.1.1 Eavesdropping 7

3.1.2 Network Vulnerabilities 8

3.1.3 Software Flaws and malware 8

3.1.4 Other Voice Service Related Threats 8

4.0 SECURING VoIP COMPONENTS **9**

4.1 VoIP Security Mechanisms *9*

4.2 Authentication *9*

4.3 Virus Protection *9*

4.4 Disabling Undesirable VoIP Features *9*

4.5 Monitoring of System Configuration Change *9*

5.0 SECURING VoIP Networks **10**

5.1 Voice and Data Separation *10*

5.2 Data Protection *10*

5.3 Firewalls *10*

5.4 URL *10*

5.5 Logs *11*

5.6 Configuration Control *11*

5.7 Physical Security *11*

5.8 Security Assessment *11*

5.9 Security Incident Response *11*

6.0 Communication Service Convergence – Unified Communications **11**

Appendix A: Checklist for Securing VoIP Systems **13**

Appendix B: Referenced Publications **16**

Appendix C: Acronyms and Definitions **17**

1.0 INTRODUCTION

This document provides techniques and procedures for the secure use of Voice over Internet Protocol (VoIP) within the Department of Homeland Security (DHS) Information Technology (IT) Program. It is published as an Attachment to the *DHS 4300A Sensitive Systems Handbook*, which is based on DHS Sensitive Systems Policy Directive 4300A.

DHS Components should use the guidance in this Handbook Attachment as a foundation for developing and implementing VoIP IT related security programs. This Attachment incorporates many security techniques and procedures already in use by DHS Components and other Federal entities such as the National Institute of Standards and Technology (NIST), the Department of Defense (DoD), and communication standardization organizations; and general VoIP security best practices commonly recommended and followed by private industry and academic communities.

1.1 Purpose and Scope

The guidance outlined in this document is intended to address security policy requirements pertinent to VoIP, and to provide a detailed explanation of security threats and corresponding countermeasures that can be applied to VoIP systems deployed by DHS Components. The security checklist in Appendix A provides a summary of VoIP security guidelines.

Authorizing Officials (AO) should understand the risks associated with each particular VoIP system, and apply some or all of the countermeasures outlined in this Attachment. They should ensure that each risk is measured and mitigated to an acceptable level according to DHS IT security policies defined by the DHS Sensitive Systems Policy Directive 4300A and other related directives.

1.2 VoIP Security Requirements Checklist

Use the Security Requirements Checklist for VoIP Systems, Appendix A to this document, to ensure Component compliance with Policy Directive 4300A and with underlying Government directives. The Checklist items identified as “Required” must be implemented by Component policies, SOPs, or other methodological documents; furthermore, implementation of the items identified as “Recommended” or equivalent provisions, will ensure that Components are compliant with best security practices.

2.0 VoIP System Overview

This section gives a brief introduction of VoIP system architecture and technologies in an enterprise environment, and provides a high-level summary of Federal guidance and policies for VoIP systems.

2.1 VoIP System Architecture

VoIP is a technology that converts voice into digital data packets that are transmitted over IP data networks such as enterprise networks or the Internet. VoIP is a mature technology that has been

widely deployed across public and private sectors since it uses existing IP data network infrastructure, eliminating expensive traditional dedicated voice circuits. The following diagram describes typical enterprise VoIP system architecture and key system components.

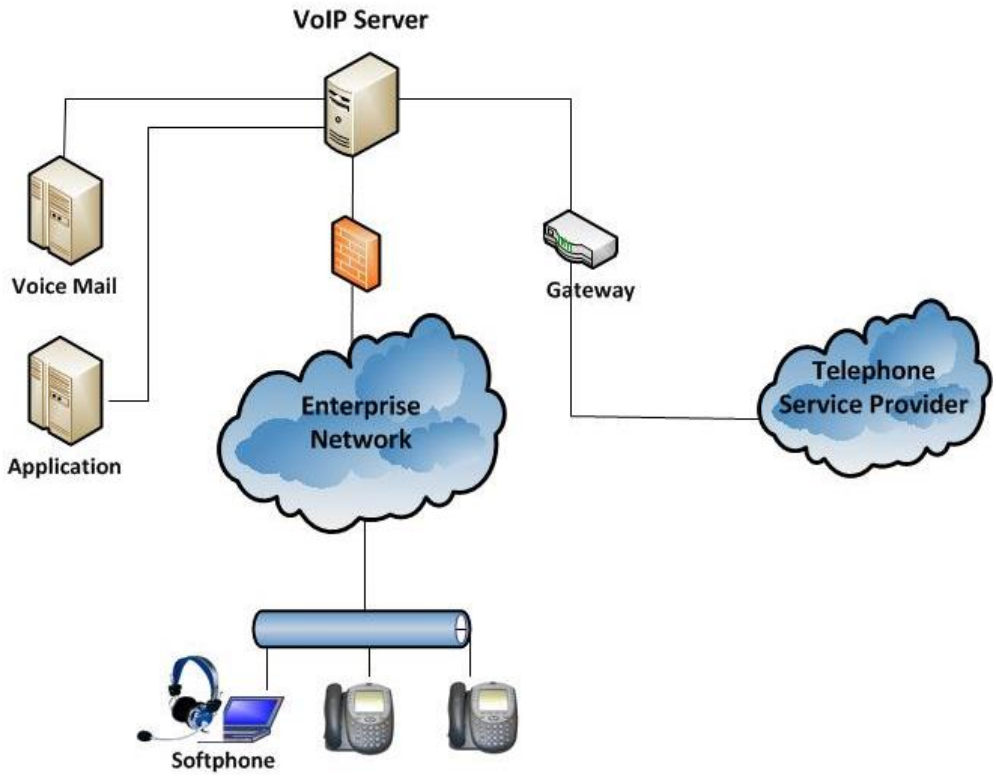


Figure 1: Enterprise VoIP System Architecture

.

The VoIP server is the control and management hub of all VoIP components. It is responsible for VoIP call session management, voice mail management, directory assistance, and other additional services such as conference bridge.

The gateway is connected to telephone service providers' Public Switched Telephone Networks (PSTN), and is the bridge between the internal VoIP system and general PSTN: all calls to or from outside telephone numbers go through the gateway.

In addition to VoIP telephone instrument hardware, VoIP softphones are widely deployed. A VoIP softphone is a computer program that runs on desktop or laptop computers, mobile devices etc., allowing users to make VoIP calls through those devices.

2.2 Federal Guidance and Polices

The U.S. Federal Communications Commission (FCC) requires VoIP systems to support enhanced 911 (E911) emergency services that provide caller identification and location information to the answering Public Safety Answering Point (PSAP).

NIST Special Publication 800-58, "Security Considerations for Voice over IP Systems," provides agencies with guidance for establishing secure VoIP networks and makes several recommendations to establish a secure VoIP and data network. Key recommendations are as follows:

- Develop appropriate network architecture.
- Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.
- Carefully consider such issues as level of knowledge and training in the technology; maturity and quality of security practices; controls, policies, and architectures; and understanding of associated security risks.
- Be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.
- Enable, use, and routinely test the security features that are included in VoIP systems.
- Deploy VoIP-ready firewalls and other appropriate protection mechanisms.
- If mobile units are to be integrated with the VoIP system, use products that implement Wi-Fi Protected Access (WPA), rather than Wired Equivalent Privacy (WEP).
- Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

3.0 THREAT OVERVIEW

This section discusses VoIP threats and vulnerabilities in an enterprise environment, and outlines corresponding countermeasures and security best practices.

3.1 VoIP Threats and Vulnerabilities

VoIP systems are vulnerable to specifically engineered attacks as well as to general network attacks. VoIP is fundamentally different from the traditional circuit-based telephony, and these differences introduce significant security threats and vulnerabilities.

A VoIP system is part of the overall enterprise IT infrastructure and is directly connected to the enterprise core IP network. Therefore strict security controls and governance must be developed and enforced by Components to mitigate constant and ever- increasing threats to DHS IT infrastructure and resources.

3.1.1 Eavesdropping

Eavesdropping describes the threat whereby an attacker secretly captures data. Eavesdropping on conventional telephone transmissions requires physical access to tap a telephone line or Private Branch Exchange (PBX). With VoIP, the eavesdropping attack surface increases dramatically: besides telephone lines and PBX, any network node or line can be tapped to capture the VoIP data (and thereby the phone conversation). Many packet capture tools (also known as packet analyzers) are readily available, often free from open sources that can be easily deployed to record VoIP conversations.

Eavesdropping risk can be mitigated by using data encryption validated by Federal Information Processing Standard (FIPS) 140-2, mandated by the Government, for all sensitive data communications within the data network. Mobile users are required by their Rules of Behavior to use the DHS Virtual Private Network (VPN) service for remote access from locations not controlled by DHS.

A robust network and physical security will also help to mitigate the risk. Network firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) can be used to filter data traffic, monitor the network infrastructure, detect and block abnormal network traffic, and send notifications to administrators if unusual events occur. Unused network access ports should be shut down and only be activated by authorized network administrators.

3.1.2 Network Vulnerabilities

Since VoIP systems are part of the overall enterprise IP network infrastructure, they will face similar network attack vectors.

A Distributed Denial of Service (DDoS) attack on the network occurs when an attacker floods the network with bogus data packets, preventing or inhibiting legitimate users from accessing the network.

In addition, VoIP data is often prioritized over other data traffic by DDoS attacks since VoIP systems must meet a strict set of network performance requirements such as short latency and low packet loss rates. Therefore, a lot of network resources serve VoIP systems at high priority. A well-crafted DDoS attack on VoIP systems will not only severely affect voice service, but will also impair other critical network activities and services.

To counter DDoS attacks, Components must implement a comprehensive defense-in-depth security strategy to secure their networks. A robust IT security system must be implemented that includes firewalls, IDS, IPS, and VoIP-aware network monitoring and management systems.

3.1.3 Software Flaws and malware

VoIP systems have many software components. The key VoIP component, the VoIP server, is often built upon commercial operating system platforms (for example, Microsoft Windows or Linux systems). Computer-based softphones will be exposed to all kind of malware including key-loggers, Trojan horses, and others) currently experienced by end users. As a result, VoIP systems inevitably will be exposed to software flaws and potential attacks from various malware.

Regular checking for software updates and patches is essential to reduce these vulnerabilities. Automated patch handling can help in reducing the window of opportunity for intruders to exploit a known software vulnerability. Standardized enterprise anti-virus tools and VoIP-related software security management systems can also greatly mitigate software threats.

3.1.4 Other Voice Service Related Threats

Other threats to VoIP systems are similar to those to traditional telephony, such as unauthorized voice devices and endpoints attempting to connect to the system, voicemail tampering, caller ID spoofing, toll fraud, etc. Toll fraud, for example is a phone hacking scheme where a compromised VoIP system is

controlled by external attackers to route long distance or international calls through enterprise networks. This can result in substantial financial loss and legal liabilities for VoIP system owners.

Existing security measures, such as requiring strong voice passwords, security awareness training, robust logging and monitoring mechanisms, and in-depth network security are some of the effective countermeasures to protect against these threats.

4.0 SECURING VoIP COMPONENTS

A VoIP system should be considered to be a critical component of the DHS network and an extension of the DHS IP network infrastructure. Critical tasks associated with securing the system include authentication, virus protection, configuration management, continuous monitoring, and disabling unused features.

4.1 VoIP Security Mechanisms

VoIP systems support a whole set of security mechanisms either specified by or used by VoIP protocols to protect the VoIP signaling and voice data messages. Secure Session Initiation Protocol (SIP) is a security mechanism that protects VoIP signaling messages over an Internet Protocol Security (IPsec) or Transport Layer Security (TLS) encrypted channel. The Secure Real-time Transport Protocol (SRTP) provides encryption, message authentication and integrity for voice messages over the communication path.

4.2 Authentication

Identification management and authentication will be implemented to access the VoIP system.

4.3 Virus Protection

Standard anti-virus software tools, -regular software updates and patches are essential to reduce software vulnerabilities to the VoIP system.

4.4 Disabling Undesirable VoIP Features

VoIP systems provide a rich set of features such as video teleconferencing. If some features are not being used but left in default unprotected configuration, they become vulnerabilities that an attacker can exploit to access the VoIP system and the network infrastructure. Components should carefully evaluate the business and operations requirements for their VoIP services and only enable the VoIP features required. For example, unprotected File Transfer Protocol (FTP) and Trivial FTP (TFTP) are often enabled by default by some VoIP systems between the VoIP server and the end-user devices for configuration management. These features should be disabled or replaced by secured ones such as Secure File Transfer Protocol (SFTP) that provide similar functionality.

4.5 Monitoring of System Configuration Change

Information Systems Security Officers (ISSO) should implement mechanisms that periodically scan for unauthorized changes to VoIP system configurations.

5.0 SECURING VoIP NETWORKS

VoIP systems are part of overall enterprise IP network infrastructure, and they introduce a number of new elements, complications and challenges to existing network management and security. The integration of voice and data in a single network is a complex process that requires greater effort than that required for data-only networks. Critical risks that must considered when securing VoIP networks include voice and data separation, data protection, operation management, physical security, security assessment, and incident response.

5.1 Voice and Data Separation

Although voice and data share the same network infrastructure, they should be logically or physically separated into two segments in order to apply different security measures (for example, different firewall rules) to reduce the likelihood of an attacker using one segment to access the other. Other benefits of separation include easier network management and troubleshooting. Separation makes attacker success more difficult and helps to provide a layered approach to VoIP and network security.

5.2 Data Protection

Data protection security means that messages are encrypted between sending device and receiving device. VoIP telephone instruments and softphones can support encryption capabilities, and data traversing the enterprise's backbone network is also protected by FIPS 140-2 validated encryption. In addition, TLS, IPSec, VPN, and Secure Shell (SSH) are common means of providing end-to-end encryption for VoIP administrators when remotely accessing the VoIP systems.

5.3 Firewalls

A firewall helps to secure the network by inspecting inbound and outbound network traffic and only allowing pre-defined data traffic. Protocols for VoIP systems specify the traffic type that is used for voice service. For example, the Session Initiation Protocol (SIP), a VoIP signaling communications protocol, requires SIP clients to use Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) on port numbers 5060 or 5061 to connect to SIP servers and other SIP endpoints. Any signaling attempt via other port numbers should be blocked by firewalls.

5.4 URL

In some cases a VoIP endpoint will be configured with one or more Uniform Resource Locators (URLs) pointing to the locations of various servers with which they are associated such as their call controller. The use of URLs in this manner permits an endpoint to find the server it is looking for in the event the server's IP address is changed. This also permits the endpoint to locate its assigned or home call controller from a remote location on a network that is not their home network. While use of URLs adds flexibility to the system and to endpoint location, it also exposes the endpoint and the home system to DNS vulnerabilities.

5.5 Logs

Logs serve as part of the VoIP monitoring and management capabilities to ensure that VoIP systems are constantly monitored. They provide a traceable mechanism for recording communication activities and they reveal network intrusions. Access to logs should be strictly controlled to ensure their integrity.

5.6 Configuration Control

Establishing configuration requirements and baseline configurations for VoIP systems can help ensure that they are deployed in a secure manner in accordance with DHS security policies.

VoIP systems are usually initially configured with default vendor settings that are common knowledge. These settings can include network information such as default channels; modulation specifications; security information such as network name, encryption methods, pass phrases or keys; and systems management information such as administration usernames, passwords, management port numbers, and default application services running.

5.7 Physical Security

Routine inspections and surveillance to detect suspicious behavior will reduce the likelihood of unauthorized equipment tampering and theft. Because VoIP end user equipment is susceptible to physical tampering, users should report any suspicious individuals or activities to appropriate security personnel.

5.8 Security Assessment

Regular security assessments should be performed to evaluate the security posture of VoIP systems and to determine corrective actions needed to ensure that the systems remain secure. Regular assessments help to determine whether VoIP systems are communicating correctly and are on correct channels. Assessments can also help Components determine whether controls are appropriately designed and operating effectively to achieve organizational control objectives. The *DHS 4300A Sensitive Systems Handbook* describes assessment areas and procedures in great detail.

5.9 Security Incident Response

Most security controls are designed to protect an organization against security threats; regardless of how effective those controls are, some security incidents are inevitable, and organizations need to have an effective response capability in place before they occur. *DHS 4300A Sensitive Systems Handbook,* Attachment F, “Incident Response” covers incident response in detail

6.0 COMMUNICATION SERVICE CONVERGENCE – UNIFIED COMMUNICATIONS

The convergence of voice, video, and data services, also referred as Unified Communications (UC), has been gaining popularity in both public and private sectors. UC integrates voice, video,

teleconferencing, messaging, email, and other enterprise applications to meet the critical and ever-increasing demand for an efficient and effective enterprise communications service.

Unlike isolated traditional voice or video systems, the UC presents an attack surface and associated vulnerabilities that have increased substantially; threats can originate from many sources: network, individual communication system, Web, the array of end-user devices, social engineering, etc. UC's integration brings greater complexity to system architecture. In addition, UC systems must address increased regulatory requirements for privacy, confidentiality, and other Government mandates such as E911 and the Health Insurance Portability and Accountability Act (HIPAA). All these factors increase the difficulty of securing UC systems.

Conventional network security measures, such as a firewall at the network boundary, help to mitigate UC risks, but are not adequate, since they are neither designed to protect UC-specific attacks nor are they aware of the complicated interaction among different UC components, and do not provide an integrated security capability for voice, video and other communication channels. An integrated security mechanism for UC is required to protect network, communication system, enterprise application and data, and end-user device in a seamless fashion. In addition, the new UC security mechanism needs to work in conjunction with existing network security measures to provide layered protection of UC systems.

APPENDIX A: CHECKLIST FOR SECURING VOIP SYSTEMS

SECURITY REQUIREMENTS CHECKLIST FOR VOIP SYSTEMS			
SECTION 4.0: SECURING VOIP COMPONENTS			
	Section 4.1: VoIP Security Mechanisms	**Required**	**Recom-mended**
	The Secure Session Initiation Protocol and Secure Real-time Transport Protocol are enabled to protect the VoIP systems.	X	
	From locations not physically controlled by DHS, users access DHS systems only via the DHS Virtual Private Network (VPN) service	X	
	Section 4.2: Authentication	**Required**	**Recom-mended**
	No password is required to access the end user VoIP phone sets.		X
	Passwords used by administrators to access key VoIP system components follow the password strength guidance given in *DHS 4300A Sensitive Systems Handbook* Section 5.1.1.1, "Selecting Strong Passwords."	X	X
	Passwords to access key VoIP system components by administrators are combined with the use of a smart card or a biometrics authentication method.		X
	Numerical passwords used for the VoIP voicemail access contain a minimum of eight digits, or the maximum allowed by the system is used if the device's maximum is less than eight.	X	
	Section 4.3: Virus Protection	**Required**	**Recom-mended**
	Anti-virus software is deployed, centrally managed, and continuously updated on VoIP systems.	X	
	Section 4.4: Disabling Undesirable VoIP Features	**Required**	**Recom-mended**
	Unapproved or unnecessary VoIP features are disabled or removed whenever possible.	X	
	Device-integrated capabilities such as cameras and recording mechanisms are subject to the approval of the AO. These capabilities have varying degrees of risk and are disabled unless specifically required, in order to mitigate the risk of exposing sensitive information		X
	End user VoIP telephone sets issued by Components are distributed and restricted to an approved baseline configuration.	X	

SECURITY REQUIREMENTS CHECKLIST FOR VOIP SYSTEMS			
⍰	**Section 4.5: Monitoring of System Configuration Change**	**Required**	**Recom-mended**
	Integrity verification mechanisms are deployed to perform system configuration integrity checks automatically, by means such as routinely comparing a cryptographic hash of the current system configuration files to a previously recorded hash known to be valid.		X
	SECTION 5.0: SECURING THE VOIP NETWORKS⍰		
⍰	**Section 5.1: Voice and Data Separation**	**Required**	**Recom-mended**
	Voice and data are logically or physically separated across the enterprise network. Common traffic separation techniques include IPSec tunnels or Virtual Local Area Network (VLAN) separation mechanisms.	X	
	A different, dedicated, IP address block or range is defined for the VoIP system that is separate from the IP address blocks/ranges used by the rest of the data network.	X	
	If the VoIP system design uses Dynamic Host Configuration Protocol (DHCP) for VoIP initial endpoint address assignment or configuration, a different and dedicated DHCP server is used than that used for data components and hosts.		X
	In the event Domain Name System (DNS) is used in the VoIP system, a different and dedicated DNS server is used and any VoIP DNS server interaction with other DNS servers is limited.		X
⍰	**Section 5.2: Data Protection**	**Required**	**Recom-mended**
	VoIP data traversing the DHS backbone network is encrypted with the FIPS 140-2 validated Advanced Encryption Standard [AES]-256 encryption to protect the confidentiality of data.	X	
	Remote access to the VoIP system uses FIPS 140-2 validated AES-256 encryption to ensure secure access.	X	
⍰	**Section 5.3: Firewalls**	**Required**	**Recom-mended**
	Firewalls for VoIP systems allow only the pre-defined VoIP traffic and block all other traffic.	X	
⍰	**Section 5.4: URL**	**Required**	**Recom-mended**
	VoIP endpoint limits the use of URLs.		X

SECURITY REQUIREMENTS CHECKLIST FOR VOIP SYSTEMS			
☐	**Section 5.5: Logs**	**Required**	**Recom-mended**
	VoIP systems are configured to create logs and capture important events such as successful and unsuccessful administrator login attempts, user attempts, device MAC and IP addresses, access violations, ports and protocols used, and application activities.	X	
	VoIP log entries are captured, analyzed, and correlated by a centralized log management system.	X	
☐	**Section 5.6: Configuration Control**	**Required**	**Recom-mended**
	Configuration requirements and baselines are established for VoIP systems in accordance with DHS security policies.	X	
	All sensitive settings for VoIP systems are changed from vendor defaults to protect against unauthorized intrusion and modification of system settings.	X	
☐	**Section 5.7: Physical Security**	**Required**	**Recom-mended**
	Users are made aware of the importance of VoIP devices and the likelihood of potential theft or tampering, able to recognize signs of tampering or attempts by unauthorized individuals to access the devices.		X
☐	**Section 5.8: Security Assessment**	**Required**	**Recom-mended**
	Annual security assessments are performed to assess VoIP system security capabilities and to discover any potential vulnerability components.	X	
☐	**Section 5.9: Security Incident Response**	**Required**	**Recom-mended**
	The security incident response standard operating procedures (SOP) specifies methods for VoIP system users and other personnel to report security incidents in accordance with DHS Sensitive Systems Policy Directive 4300A.	X	

APPENDIX B: REFERENCED PUBLICATIONS

DHS Publications

ISSM Guide to the DHS Information Security Program, Version 2.0, July 19, 2004,

ISSO Guide to the DHS Information Security Program, Version 0.6, July 26, 2004

DHS Sensitive Systems Policy Directive 4300A, Version 9.1, July 24, 2012

DHS Sensitive Systems Handbook, Version 9.1, July 24, 2012

"IT Security Architecture Guidance Volume I: Network and System Infrastructure," Version 2.0, 2005
http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Documents/Information%20Security%20Architecture%20Guidance%20vol%201.doc

"IT Security Architecture Guidance Volume II: Security Operations Support," Version 2.0, 2005
http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Documents/Information%20Security%20Architecture%20Guidance%20vol%202.doc

"IT Security Architecture Guidance Volume III: Application Infrastructure Design (Draft), ver. 1.0, 2005
http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Documents/Information%20Security%20Architecture%20Guidance%20vol%203.doc

Defense Information Systems Agency (DISA) Publications

Wireless Security Technical Implementation Guide (STIG), and Addendums
Current versions at: http://iase.disa.mil/stigs/net_perimeter/telecommunications.voip.html

National Institute of Standards and Technology (NIST) Publications

NIST SP 800-58, "Security Considerations for Voice Over IP Systems," January 2005

NIST SP 800-53, Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013

National Security Agency (NSA) Publications

National Security Agency / Central Security Service Web Site, http://www.nsa.gov

Committee on National Security Systems (CNSS) Instructions

CNSS Instruction No. 4009 (Revised), "National Information Assurance Glossary," April 2010

Other Publications

FAQS.ORG, Network Working Group, "Request for Comments (RFC) 2828, Internet Security Glossary" http://www.faqs.org/rfcs/rfc2828.html

SANS Institute, "VoIP Security Vulnerabilities." 2007

APPENDIX C: ACRONYMS AND DEFINITIONS

Acronym	Definition
AES	Advanced Encryption Standard
AO	Authorizing Official
ATO	Authority to Operate
C&A	Certification and Accreditation
CISO	Chief Information Security Officer
CSIRC	Computer Security Incident Response Center
DAA	Designated Approving Authority
DHS	Department of Homeland Security
DDOS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoD	Department of Defense
E911	Enhanced 911
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
MAC	Media Access Control
IPsec	Internet Protocol Security
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Science and Technology
NSA	National Security Agency
OSI	Open Systems Interconnection
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
RTP	Real-time Protocol
SIP	Session Initiation Protocol

Acronym	Definition
SOP	Standard Operating Procedure
SRTP	Secure Real-time Protocol
SSH	Secure Shell
SSIP	Secure Session Initiation Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

U.S. CUSTOMS AND BORDER PROTECTION

ATTACHMENT Q6

BLUETOOTH SECURITY

HB 1400-05D

INFORMATION SYSTEMS SECURITY POLICIES AND PROCEDURES HANDBOOK

VERSION
7.0

November 16, 2017

This page intentionally blank

Document Change History

Version	Date	Description
4.0	December 15, 2014	Initial Version.
5.3	April 6, 2015	Final Version
6.0	March 3, 2016	No Changes.
6.01	May 17, 2016	No Changes.
6.02	September 2016	No Changes.
7.0	November 16, 2017	No Changes.

.

CONTENTS

1.0 Introduction **1**

1.1 Authority *1*

1.2 Purpose and Scope *1*

1.3 Background *1*

1.4 Homeland Security Mission-Driven Use Cases *2*

2.0 Requirements of DHS Policy Directive 4300A **3**

3.0 Bluetooth Threats and Vulnerabilities **3**

4.0 Bluetooth Security Modes **4**

4.1 Security Mode 1 ..... *4*

4.2 Security Mode 2 ..... *4*

4.3 Security Mode 3 ..... *4*

4.4 Security Mode 4 ..... *5*

5.0 Bluetooth Device Communication Risks And Recommendations **5**

5.1 Management Best Practices *5*

5.2 Technical Best Practices *6*

5.3 Operational and Deployment Best Practices *7*

6.0 Compliant Bluetooth Product Lists **8**

INTRODUCTION

This document provides techniques and procedures for securely implementing Bluetooth enabled devices and peripherals in the Department of Homeland Security (DHS). The intent is to assure a minimum-security baseline when installing, configuring, using, and managing Bluetooth-capable devices. In mitigating risks posed by the use of Bluetooth enabled devices, the approach should be holistic; security controls for the host environment and Bluetooth device work together to reduce the risk of loss of confidentiality, availability, integrity, and non-repudiation.

Authority

This document is issued as implementation guidance under the authority of the DHS Chief Information Officer (CIO) through the DHS Office of the Chief Information Security Officer (OCISO).

Purpose and Scope

This document addresses the security specifics of sensitive wireless systems only and does not cover the use of classified wireless systems. DHS Sensitive Systems Policy Directive 4300A prohibits use of wireless communications technologies throughout DHS unless the appropriate Authorizing Official (AO) specifically approves the technology and the application. AOs must also approve the implementation and use of wireless systems at a specified risk level during the security authorization process and ensure appropriate and effective security measures are included in the Security Plan. This document sets forth acceptably secure configurations and applications of Bluetooth wireless communications that offer mechanisms and conditions under which AOs can approve limited Bluetooth use, and associated risk level specifications.

Background

Bluetooth is a wireless open standard technology used for exchanging voice or data over short distances between devices without interconnecting cables. Effective range varies and depends on propagation conditions, material coverage, antenna configuration, battery condition, etc., but most Bluetooth devices have an effective range of 10m (33 ft.) or less. The technology has been integrated into many types of devices including cell phones, laptops, printers, keyboards, mice, and headsets, and is used primarily to establish ad hoc wireless personal area networks (WPANs) – also known as *piconets* – between devices (for example, a connection between a cell phone and a headset), as shown in Figure 1.

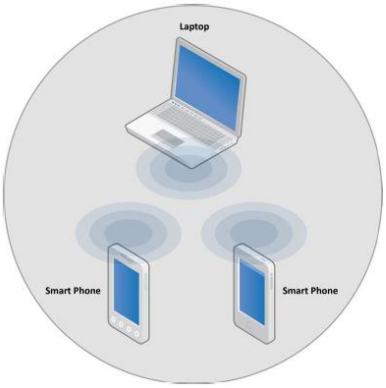


Figure 1: Ad hoc *Bluetooth network*

Bluetooth versions 1.1 and 1.2 only support transmission speeds up to 1 megabit per second (Mbps), known as Basic Rate (BR), and can achieve payload throughput of approximately 720 kilobits per second (kbps). Enhanced Data Rate (EDR), introduced in version 2.0, specifies data rates up to 3 Mbps and throughput of approximately 2.1 Mbps.

Devices connect under a master-slave structure, a model of communication where the master device or process has unidirectional control over one or more other devices. A master Bluetooth device, such as a smartphone or tablet, may communicate with up to seven (7) devices in a piconet, (e.g. other smartphones, headsets, keyboards, printers, etc.), although not all devices reach this maximum. In some cases the devices may switch roles and a slave becomes the master (for example, a headset initiating a connection to a phone may initially serve as master, as initiator of the connection; but may later prefer to serve as slave once the connection is established).

The Bluetooth Core Specification provides for connection of two or more piconets to form a *scatternet* in which certain devices simultaneously function as master in one piconet and as slave in another.

Except in the seldom used broadcast mode, data is being transferred between two devices. The master selects which slave to address, typically switching rapidly from one device to another in a round-robin fashion.

Homeland Security Mission-Driven Use Cases

The following are examples in which use of Bluetooth technology could enhance the ability of Department personnel to fulfill their mission and business requirements. Examples are based on mission-driven use cases; the list is not exhaustive.

- Bluetooth keyboard for tablets in office environments (data)
- Officer earpieces enabling hands free inspections, protective details, border security missions (voice)
- Bluetooth headset for office workers (voice)

Bluetooth Personal Identity Verification (PIV) card readers (data)

Hands free mobile phone use in a vehicle (voice)

Field operations in degraded or failed communications infrastructure (voice and data)

Transfer of data between a mobile device and a base unit at an inspection point (data)

Collection of fingerprints from suspects or persons of interest encountered in the field during law enforcement encounters or investigations (data – Personally Identifiable Information)

REQUIREMENTS OF DHS POLICY DIRECTIVE 4300A

Wireless systems include wireless local area networks (WLAN), wireless wide area networks (WWAN), wireless personal area networks (WPAN) such as Bluetooth, peer-to-peer wireless networks (i.e., ad hoc wireless networks), and systems that leverage commercial wireless services. Wireless systems include the transmission medium, stationary integrated devices, firmware, supporting services, and protocols. *DHS Sensitive Systems Policy Directive 4300A* establishes the Department's wireless systems policies. System owners should submit the documentation required by policy to the appropriate AO.

BLUETOOTH THREATS AND VULNERABILITIES

Bluetooth has clear ease of use advantages compared to cabled devices and peripherals, but like any wireless technology, Bluetooth communications are susceptible to a variety of threats. The technology has been fielded using a wide variety of chipsets, operating systems, and physical device configurations resulting in a large number of differing security programming interfaces and default settings. These complexities, added to those of wireless communications in general, mean that Bluetooth is susceptible to general wireless threats as well as having its own inherent vulnerabilities. Bluetooth is a peer-to-peer network technology that lacks a centralized security enforcement infrastructure. The Bluetooth specification is very complex and includes support for many voice and data services such as headset, data transfer, printing, and others. Common attacks include:

- Bluebugging – Attacker takes control of phone; can make and take calls, listen to phone conversations, read contacts and calendars
- Bluejacking – Sends anonymous, unsolicited messages to phones with Bluetooth set to discoverable
- Blueprinting – A method to remotely fingerprint Bluetooth-enabled devices
- BlueSmack – Performs a denial of service attack over the Bluetooth connection making the device unavailable
- Bluesnarfing– Gives attacker full access to calendar, contacts, e-mail and text messages
- BlueStumbling – Allows an adversary to locate and identify users based on their Bluetooth device addresses

BLUETOOTH SECURITY MODES

The Bluetooth specification includes four security modes. This section provides an overview and application for each. Security Mode 3 provides the best security.

Security Mode 1

Security Mode 1 devices are not considered to be secure. Security functionality (authentication and encryption) is never initiated; therefore the device and connections are susceptible to attack. In effect, Bluetooth devices in this mode are "indiscriminate" and do not employ any mechanisms to prevent other Bluetooth-enabled devices from establishing connections. If a remote device initiates pairing, authentication, or encryption request, a Security Mode 1 device will accept without authenticating the request. Per their respective Bluetooth specification versions, all v2.0 and earlier devices can support Security Mode 1, and v2.1 and later devices can use Security Mode 1 for backward compatibility with older devices. Because of its high vulnerability, Security Mode 1 shall not be used by DHS.

Security Mode 2

Security Mode 2 is service level enforced in which security procedures may be initiated after link establishment but before logical channel establishment. In this security mode, a local security manager (specified in the Bluetooth architecture) controls access to specific services. Firmware maintains policies for access control and interfaces with other protocols and device users. Varying security policies and trust levels to restrict access can be defined for applications with different security requirements operating in parallel. It is possible to grant access to some services without providing access to other services. In this mode, the notion of authorization—the process of deciding whether a specific device is allowed to have access to a specific service—is introduced. Typically Bluetooth service discovery can be performed prior to any security challenges (i.e., authentication, encryption, and/or authorization). All other Bluetooth services, however, should require all of those security mechanisms.

It is important to note that the authentication and encryption mechanisms used for Security Mode 2 are implemented in the controller, as with Security Mode 3 described in the following section. All v2.0 and earlier devices can support Security Mode 2, but v2.1 and later devices can only support backward compatibility with v2.0 or earlier devices.

Security Mode 3

Security Mode 3 provides the best security. It is the link level enforced security mode, in which a Bluetooth device initiates security procedures before the link is fully established. Bluetooth devices operating in Security Mode 3 mandate authentication and encryption for all connections to and from the device. Therefore, not even service discovery can be performed before authentication, encryption, and authorization have been performed. A service level authorization is not typically performed by a Security Mode 3 device once the device has been authenticated. Service-level authorization should be performed to prevent "authentication abuse," where an authenticated remote device uses a Bluetooth service without the local

device owner's knowledge. All v2.0 and earlier devices can support Security Mode 3, but v2.1 and later devices can only backward compatibility with v2.0 and later devices.

Security Mode 4

Security Mode 4 uses Secure Simple Pairing (SSP), in which Elliptic Curve Diffie-Hellman (ECDH) key agreement replaces legacy key agreement for link key generation. Device authentication and encryption algorithms, however, are identical to the algorithms in Bluetooth v2.0 + EDR and earlier versions. Security requirements for services protected by Security Mode 4 must be classified as one of the following:

Authenticated link key required

Unauthenticated link key required

No security required

Whether or not a link key is authenticated depends on the SSP association model used. Security Mode 4 requires encryption for all services except Service Discovery and is mandatory for communication between v2.1 and later Basic Rate/Enhanced Data Rate (BR/EDR) devices. However, for backward compatibility, a Security Mode 4 device can fall back to any of the other three Security Modes when communicating with Bluetooth v2.0 and earlier devices that do not support Security Mode 4. For this reason Security Mode 3 should be employed.

BLUETOOTH DEVICE COMMUNICATION RISKS AND RECOMMENDATIONS

During and after Bluetooth device pairing, critical information is passed between devices. If captured, this critical information could allow an attacker to gain full remote access to the WPAN device. For more information on Bluetooth security see NIST SP 800-121, *Guide for Bluetooth Security*.

As technology advances, so do attack vectors and methodologies. In order to reduce the risk of data compromise, the following are best practices to employ:

Management Best Practices

Ensure that Bluetooth users are made aware of their security-related responsibilities regarding Bluetooth use and provide them with a list of precautionary measures to better protect handheld Bluetooth devices from theft.

Enable Bluetooth only when necessary (e.g. turn off Bluetooth on the mobile device and turn off the headset when not in use).

Minimize distance between Bluetooth linked devices when Bluetooth links are active.

Minimize the duration of voice calls.

Minimize opportunity for signal interception. Maximize the distance from other Bluetooth devices, other people, and untrusted areas.

When pairing, the mobile device will attempt to find other Bluetooth-enabled devices. Always verify and confirm the device being paired. Never enter passkeys when unexpectedly prompted for them.

Remove lost, stolen or unused devices from paired device list.

Perform comprehensive security assessments at regular intervals to fully understand the Bluetooth security posture.

Ensure that wireless devices and networks involving Bluetooth technology are fully understood from an architecture perspective and documented accordingly.

Maintain a complete inventory of all Bluetooth-enabled devices and addresses.

Designate an individual to track the progress of Bluetooth security products and standards and the threats and vulnerabilities with the technology.

Technical Best Practices

Change the default settings of the Bluetooth device.

Set Bluetooth devices to the lowest power level sufficient for communications, so that transmissions remain within a secure perimeter. The lowest Bluetooth power should be employed that is sufficient to maintain communications between authorized users.

Choose Personal Identity Number (PIN) codes that are sufficiently random, long and private. Avoid static and weak PINs, such as all zeroes. PIN codes should be random so that malicious users cannot easily guess them. Longer PIN codes are more resistant to brute force attacks.

Ensure that link keys are not based on unit keys. The use of shared unit keys can lead to successful spoofing, “Man in the Middle” (MITM), and eavesdropping attacks.

Avoid using the “Just Works” association model. The device must verify that an authenticated link key was generated during pairing. The “Just Works” association model does not provide MITM protection. Devices that only support “Just Works” (e.g., devices that have no input/output capability) should not be procured.

Use random and unique passkeys for each pairing, based on the Passkey Entry association model. If a static passkey is used for multiple pairings, the MITM protection provided by the Passkey Entry association model is reduced.

A Bluetooth device using Security Mode 4 must fall back to Security Mode 3 for backward compatibility with v2.0 and earlier devices (i.e., for devices that do not support Security Mode 4). The Bluetooth specifications allow a v2.1 device to fall back to any Security Mode for backward compatibility. This allows the option of falling back to Security Modes 1- 3. Security Mode 3 provides the best security.

Lock down the Bluetooth stack on every device to ensure that only required and approved profiles and services are available for use. Many Bluetooth stacks are designed to support multiple profiles and associated services. Disable unneeded and unapproved services.

Configure Bluetooth devices by default as undiscoverable and to remain undiscoverable except as needed for pairing. This prevents visibility to other Bluetooth devices except when discovery

is absolutely required. The default Bluetooth device names sent during discovery should be changed to non-identifying values.

Invoke link encryption for all Bluetooth connections, and use it to secure all data transmissions during Bluetooth connections; otherwise, transmitted data is vulnerable to eavesdropping.

If multi-hop wireless communication is being used, ensure that encryption is enabled on every link in the communication chain. One unsecured link results in compromise of the entire communication chain.

Ensure that mutual device authentication is performed for all connections. Mutual authentication is required to provide verification that all devices on the network are legitimate.

Enable encryption for all broadcast transmissions (Encryption Mode 3). Broadcast transmissions secured by link encryption provide a layer of security that protects these transmissions from interception for malicious purposes.

Configure encryption key sizes to the maximum allowable (128-bit). Using maximum allowable key sizes provides protection from brute force attacks.

Use additional application-level authentication and encryption atop the Bluetooth stack for sensitive data communication. Bluetooth devices can access link keys from memory and automatically connect with previously paired devices. Incorporating application level software that implements authentication and encryption will add an extra layer of security. Employing higher layer encryption (particularly Federal Information Processing Standards [FIPS] 140 validated) over the native encryption will further protect the data in transit.

Operational and Deployment Best Practices

Ensure that Bluetooth capabilities are disabled when they are not in use. Bluetooth capabilities should be disabled on all devices, except when the user explicitly enables Bluetooth to establish a connection. This minimizes exposure to potential malicious activities. For devices that do not support disabling Bluetooth (e.g., headsets), the entire device should be turned off when not in use. Perform pairing as infrequently as possible, ideally in a secure area where attackers cannot realistically observe the passkey entry or intercept Bluetooth pairing messages. Users should not respond to any messages requesting a PIN unless the user has initiated a pairing and is certain the PIN request is being sent by one of the user's devices. Pairing is a vital security function and requires that users maintain a security awareness of possible eavesdroppers.

A BR/EDR service-level security mode (i.e., Security Mode 2 or 4) should only be used in a controlled and well-understood environment. Security Mode 3 provides the best security.

Ensure that portable devices with Bluetooth interfaces are configured with a password or access PIN enabled. This helps prevent unauthorized access if the device is lost or stolen.

If a Bluetooth device is lost or stolen, users should immediately delete the missing device from the paired device lists of all other Bluetooth devices.

Install antivirus software on Bluetooth-enabled hosts that support such host-based security software.Fully test and regularly deploy Bluetooth software and firmware patches and

upgrades.Do not accept transmissions of any kind from unknown or suspicious devices. These types of transmissions often include messages, files, and images.

Fully understand the impacts of deploying any security feature or product prior to deployment.

COMPLIANT BLUETOOTH PRODUCT LISTS

General Services Administration (GSA) operates and maintains the FIPS 201 Evaluation Program (EP) and its Approved Products List (APL), as well as services for Federal Identity, Credentialing and Access Management (FICAM) segment architecture conformance and compliance. As part of the FICAM Testing Program, GSA manages the APL. This list provides Federal agencies with the products and services related to ICAM implementation that have been approved based on testing done by the FICAM Testing Program. This list includes Bluetooth Fingerprint Scanners and Bluetooth Smart Card Readers.

U.S. CUSTOMS AND BORDER PROTECTION

ATTACHMENT R
COMPLIANCE FRAMEWORK FOR CFO-DESIGNATED SYSTEMS

HB 1400-05D

INFORMATION SYSTEMS SECURITY POLICIES AND PROCEDURES HANDBOOK

VERSION
7.0

NOVEMBER 16, 2017

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	Updated and aligned content with the revised GAO Federal Information System Control Audit Manual (FISCAM), NIST SP800- 53 Rev.3, and DHS Sensitive Systems Policy Directive 4300A, Version 7.1.
3.0	February 8, 2012	No Changes.
4.0	May 10, 2013	Edited for style, grammar, and format.
5.0	May 10, 2014	No Changes.
6.0	March 3, 2016	No Changes.
6.01	May 17, 2016	No Changes.
6.02	September 2016	Section 2.4 under Documentation - Changed reference from TAF to IACS.
7.0	November 16, 2017	No Changes.

THIS PAGE INTENTIONALLY BLANK

TABLE OF CONTENTS

1.0 INTRODUCTION 1

2.0 COMPLIANCE ACTIVITIES BY FISCAM DOMAIN 2

2.1 SECURITY MANAGEMENT 2

2.1.1 SM COMPLIANCE ACTIVITIES 2

2.2 ACCESS CONTROLS 5

2.2.1 AC COMPLIANCE ACTIVITIES 5

2.3 CONFIGURATION MANAGEMENT 12

2.3.1 CM COMPLIANCE ACTIVITIES 12

2.4 CONTINGENCY PLANNING 15

2.5 SEGREGATION OF DUTIES 16

2.5.1 SD COMPLIANCE ACTIVITIES 16

1.1 INTRODUCTION

DHS CHIEF FINANCIAL OFFICER (CFO) DESIGNATED SYSTEMS ARE SYSTEMS THAT REQUIRE ADDITIONAL MANAGEMENT ACCOUNTABILITY TO ENSURE EFFECTIVE INTERNAL CONTROL EXISTS OVER FINANCIAL REPORTING. THE DHS CFO PUBLISHES THE APPROVED LIST OF CFO DESIGNATED SYSTEMS ANNUALLY. SECTION 3.15 OF DHS SENSITIVE SYSTEMS POLICY DIRECTIVE 4300A PROVIDES ADDITIONAL REQUIREMENTS FOR THESE SYSTEMS BASED ON OFFICE OF MANAGEMENT AND BUDGET (OMB) CIRCULAR NO. A-123, "MANAGEMENT'S RESPONSIBILITY FOR INTERNAL CONTROL", APPENDIX A, "IMPLEMENTATION GUIDE, INTERNAL CONTROL OVER FINANCIAL REPORTING, UNDERSTANDING THE IT INFRASTRUCTURE AND ASSOCIATED RISKS."

OMB A-123 APPENDIX A DEFINES INFORMATION TECHNOLOGY GENERAL CONTROLS (ITGC), CONTROLS THAT ADDRESS STRUCTURE, POLICIES, AND PROCEDURES RELATED TO AN ENTITY'S OVERALL COMPUTER OPERATIONS. ITGCS ARE NOT TIED TO ANY ONE BUSINESS PROCESS, BUT MAY BE RELATED TO A NUMBER OF APPLICATIONS, ASSOCIATED TECHNICAL INFRASTRUCTURE ELEMENTS, AND INFORMATION SYSTEMS MANAGEMENT ORGANIZATIONS THAT SUPPORT LINE OF BUSINESS PROCESSES.

THE *FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL* (FISCAM), WHICH PROVIDES GUIDANCE ON HOW TO INCORPORATE ROBUST AND SECURE FINANCIAL AUDITING CONTROLS, IS USED TO ASSESS ITGCS.

IN ACCORDANCE WITH OMB A-123 APPENDIX A, THE FOLLOWING FIVE DOMAINS ARE REQUIRED IN THE ASSESSMENT ITGCS:

- SECURITY MANAGEMENT (SM)
- ACCESS CONTROLS (AC)
- CONFIGURATION MANAGEMENT (CM)
- CONTINGENCY PLANNING (CP)
- SEGREGATION OF DUTIES (SD)

TO SUPPORT THIS REQUIREMENT, THE DHS CISO DEVELOPED THE COMPLIANCE FRAMEWORK FOR CFO DESIGNATED SYSTEMS. THE FRAMEWORK MAPS THE RELEVANT NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) SPECIAL PUBLICATION (SP) 800-53 REVISION 3 CONTROLS TO THE FIVE FISCAM DOMAINS IDENTIFIED ABOVE AND IDENTIFIES THE COMPLIANCE ACTIVITIES THAT SHOULD BE PERFORMED EACH YEAR TO ADDRESS THE DOMAINS. THE CFO DESIGNATED SYSTEMS REQUIREMENTS ARE IN ADDITION TO THE OTHER FINANCIAL SYSTEM LINE OF BUSINESS REQUIREMENTS DEVELOPED BY THE CFO.

THESE ADDITIONAL REQUIREMENTS PROVIDE A STRENGTHENED ASSESSMENT PROCESS AND FORM THE BASIS FOR MANAGEMENT'S ASSURANCE OF INTERNAL CONTROL OVER FINANCIAL REPORTING. THE STRENGTHENED PROCESS REQUIRES MANAGEMENT TO DOCUMENT THE DESIGN AND TO TEST THE OPERATING EFFECTIVENESS OF CONTROLS FOR CFO DESIGNATED SYSTEMS.

THE SYSTEM OWNER IS RESPONSIBLE FOR ENSURING THAT ALL REQUIREMENTS, INCLUDING SECURITY REQUIREMENTS, ARE IMPLEMENTED ON DHS SYSTEMS. COMPONENT CHIEF INFORMATION SECURITY OFFICERS (CISOS) AND INFORMATION SYSTEM SECURITY MANAGERS (ISSMS) MUST COORDINATE WITH THEIR CFO ORGANIZATION TO ENSURE THAT REQUIREMENTS ARE MET.

2.0 COMPLIANCE ACTIVITIES BY FISCAM DOMAIN

2.1 SECURITY MANAGEMENT

SECURITY MANAGEMENT CONTROLS PROVIDE REASONABLE ASSURANCE THAT SECURITY MANAGEMENT IS EFFECTIVE IN THE FOLLOWING AREAS:

- SECURITY MANAGEMENT PROGRAM
- PERIODIC ASSESSMENTS AND VALIDATION OF RISK
- SECURITY CONTROL POLICIES AND PROCEDURES
- SECURITY AWARENESS TRAINING AND OTHER SECURITY-RELATED PERSONNEL ISSUES
- PERIODIC TESTING AND EVALUATION OF THE EFFECTIVENESS OF INFORMATION SECURITY POLICIES, PROCEDURES, AND PRACTICES
- REMEDIATION OF INFORMATION SECURITY WEAKNESSES
- SECURITY OVER ACTIVITIES PERFORMED BY EXTERNAL THIRD PARTIES

2.1.1 SM COMPLIANCE ACTIVITIES

Compliance Review
Conduct the following compliance review procedures in RTM: • Plan of Action and Milestones (CA-5) • Security Authorization (CA-6) • DHS Sensitive Systems Policy Directive 4300A (PD 4300A), 3.15.e: CFO Approval • DHS PD 4300A, 3.15.j: CFO Waivers • DHS PD 4300A, 4.6.1.a: Wireless Assessments • DHS PD 4300A, 4.6.1.b: Wireless vulnerabilities • DHS PD 4300A, 4.6.1.e: Legacy Wireless • System Security Plan (PL-2) • Privacy Impact Assessment (PL-5) • DHS PD 4300A, 3.14.2.a: PTA • DHS PD 4300A, 3.14.5.a: PII 1

- DHS PD 4300A, 3.14.5.B: PII 2
- DHS PD 4300A, 3.14.5.C: PII 3
- DHS PD 4300A, 3.14.5.D: PII 4
- DHS PD 4300A, 3.15.K: CFO DESIGNATED SYSTEM ISSO
- DHS PD 4300A, 3.15.L: CFO C&A
- DHS PD 4300A, 4.8.5.A: ROB
- DHS PD 4300A, 4.8.5.E: CONSENT TO MONITOR
- DHS PD 4300A, 4.8.5.F: CONTRACTOR PRIVILEGES
- PERSONNEL SCREENING (PS-3)
- PERSONNEL TERMINATION (PS-4)
- PERSONNEL TRANSFER (PS-5)
- ACCESS AGREEMENTS (PS-6)
- THIRD-PARTY PERSONNEL SECURITY (PS-7)
- DHS PD 4300A, 4.1.1.A: POSITION SENSITIVITY
- DHS PD 4300A, 4.1.1.B: PERSONNEL SECURITY
- DHS PD 4300A, 4.1.1.C: FAVORABLY ADJUDICATION
- DHS PD 4300A, 4.1.1.D: ACCESS
- DHS PD 4300A, 4.1.1.E: ACCESS
- DHS PD 4300A, 4.1.6.B: MEDIA TRANSFER
- SECURITY CATEGORIZATION (RA-2)
- RISK ASSESSMENT (RA-3)
- DHS PD 4300A, 3.6.C: CUSTOM CODE REVIEW
- DHS PD 4300A, 3.15.A: SECURITY ASSESSMENT
- DHS PD 4300A, 3.15.C: VULNERABILITY ASSESSMENT

VULNERABILITY ASSESSMENT

MINIMUM REQUIRED TESTS FOR CFO DESIGNATED SYSTEMS:

- NONE

ADDITIONAL RECOMMENDED TESTS FOR CFO DESIGNATED SYSTEMS

- NONE

DOCUMENTATION

ENSURE THAT THE FOLLOWING DOCUMENTS ARE COMPLETE, ACCURATE, AND CURRENT:

- DHS ARTIFACTS IN TAF:
  - SYSTEM SECURITY PLAN (SSP)
  - RISK ASSESSMENT (RA)
  - PRIVACY THRESHOLD ANALYSIS (PTA)
  - PRIVACY IMPACT ASSESSMENT (PIA)
  - AUTHORITY TO OPERATE (ATO)/INTERIM ATO LETTER
  - COMPLIANCE TEST RESULTS/RTM ARTIFACT
  - VULNERABILITY ASSESSMENT RESULTS/SCAN LETTER
  - CONTINGENCY PLAN TEST RESULTS
  - PLANS OF ACTIONS & MANAGEMENT (POA&MS)
  - VALID INTERCONNECTIONS SECURITY AGREEMENT
  - MEMORANDUMS OF AGREEMENT (MOA) AND MEMORANDUMS OF UNDERSTANDING (MOU) (IF APPLICABLE)
- DOCUMENTS TO BE MANAGED BY ISSO:
  - COMPLETED RULES OF BEHAVIOR FORMS
  - POA&MS
- DOCUMENTS TO BE MONITORED BY ISSO:
  - LIST OF USER ACCOUNTS: SYSTEM GENERATED LIST OF USERS, INCLUDING DATE CREATED AND DATE OF LAST LOGON
  - LIST OF PRIVILEGED USER ACCOUNTS: SYSTEM GENERATED LIST OF SYSTEM ADMINISTRATORS, DBAS, AND APPLICATION DEVELOPERS/PROGRAMMERS, INCLUDING DATE CREATED AND DATE OF LAST LOGON
  - LIST OF TRANSFERRED OR SEPARATED EMPLOYEES AND CONTRACTORS, INCLUDING DATE OF SEPARATION AND DATE OF ACCESS REMOVAL (ACCOUNT DISABLED OR REMOVED)
  - CONTRACTOR NDAS: COPIES OF COMPLETED NON-DISCLOSURE AGREEMENTS (NDA) FOR ALL CONTRACTOR PERSONNEL
  - POA&MS

2.2 ACCESS CONTROLS

ACCESS CONTROLS (AC) PROVIDE REASONABLE ASSURANCE THAT ACCESS TO COMPUTER RESOURCES (DATA, EQUIPMENT, AND FACILITIES) IS REASONABLE AND IS RESTRICTED TO AUTHORIZED INDIVIDUALS. ACCESS CONTROLS INCLUDE EFFECTIVE:

- PROTECTION OF INFORMATION SYSTEM BOUNDARIES
- IDENTIFICATION AND AUTHENTICATION MECHANISMS
- AUTHORIZATION CONTROLS
- PROTECTION OF SENSITIVE SYSTEM RESOURCES
- AUDIT AND MONITORING CAPABILITY, INCLUDING INCIDENT HANDLING
- PHYSICAL SECURITY CONTROLS

2.2.1 AC COMPLIANCE ACTIVITIES

Compliance Review
Conduct the following compliance review procedures in RTM: • Account Management (AC-2) • Access Enforcement (AC-3) • Information Flow Enforcement (AC-4) • Least Privilege (AC-6) • Unsuccessful Login Attempts (AC-7) • System Use Notification (AC-8) • Session Lock (AC-11) • Remote Access (AC-17) • DHS PD 4300A, 4.1.3.a: Need to Know • DHS PD 4300A, 4.1.6.a: System Access • DHS PD 4300A, 4.3.1.e: Media level • DHS PD 4300A, 4.3.1.f: USB media

- DHS PD 4300A, 4.5.2.b: FAX
- DHS PD 4300A, 4.5.3.c: Teleconference
- DHS PD 4300A, 4.6.2.c: Wireless
- DHS PD 4300A, 4.6.2.l: PED Approvals
- DHS PD 4300A, 4.6.4.b: RFID
- DHS PD 4300A, 4.8.1.c: Unattended Workstations
- DHS PD 4300A, 4.8.4.b: System Access
- DHS PD 4300A, 4.8.5.c: Privacy
- DHS PD 4300A, 4.8.5.d: Consent to Monitor
- DHS PD 4300A, 4.9.a: Monitoring
- DHS PD 4300A, 5.2.a: Access Controls
- DHS PD 4300A, 5.2.b: Access Controls
- DHS PD 4300A, 5.2.d: Temp Access
- DHS PD 4300A, 5.2.e: Account Identifiers
- DHS PD 4300A, 5.2.1.a: Failed Logon Attempts
- DHS PD 4300A, 5.2.1.b: Account Lockout
- DHS PD 4300A, 5.2.1.c: Account Reset
- DHS PD 4300A, 5.2.2.a: Session Inactivity
- DHS PD 4300A, 5.2.2.b: Session Lockout
- DHS PD 4300A, 5.2.2.c: Session Inactivity II
- DHS PD 4300A, 5.4.1.a: Modem Usage
- DHS PD 4300A, 5.4.1.b: Remote Access
- DHS PD 4300A, 5.4.1.c: Remote Access of PII
- DHS PD 4300A, 5.4.1.d: Remote Access of PII 2
- DHS PD 4300A, 5.4.1.f: Remote Access PSTN
- DHS PD 4300A, 5.4.3.a: Network Security
- DHS PD 4300A, 5.4.4.a: Restrict Firewall Access

- DHS PD 4300A, 5.4.4.b: Strong Firewall I&A
- DHS PD 4300A, 5.4.4.c: Firewall Maintenance
- DHS PD 4300A, 5.4.5.f: Remote Desktop Authentication
- Auditable Events (AU-2)
- Contents of Audit Records (AU-3)
    - Audit Monitoring, Analysis, and Reporting (AU-6)
    - Protection of Audit Information (AU-9)
    - Audit Generation (AU-12)
    - DHS PD 4300A, 5.3.a Audit Trail Content
    - DHS PD 4300A, 5.3.b: Financial/PII Audit Review
    - DHS PD 4300A, 5.3.c: Audit Records and Logs Protection
    - DHS PD 4300A, 5.3.e: Risks from PII
    - DHS PD 4300A, 5.3.f: Threat-specific logging
    - Identifier Management (IA-4)
    - Authenticator Management (IA-5)
    - DHS PD 4300A, 3.14.7.a: E-Authentication
    - DHS PD 4300A, 3.14.7.b: E-Authentication
    - DHS PD 4300A, 3.14.7.c: E-Authentication
    - DHS PD 4300A, 4.3.1.d: Encryption
    - DHS PD 4300A, 4.6.b: Wireless PKI
    - DHS PD 4300A, 4.6.4.f: RFID
    - DHS PD 4300A, 5.1.c Disable USERID
    - DHS PD 4300A, 5.1.d: I & A
    - DHS PD 4300A, 5.1.1.a: Strong Passwords
    - DHS PD 4300A, 5.1.1.b: Password Aging
    - DHS PD 4300A, 5.1.1.c: Password Sharing
    - DHS PD 4300A, 5.1.1.d: Group Passwords
    - DHS PD 4300A, 5.1.1.e: Scripted Passwords

- DHS PD 4300A, 5.1.1.f: Encrypted Passwords
- DHS PD 4300A, 5.1.1.3: Account Name Restriction
- DHS PD 4300A, 5.1.1.3: Account Validation
- DHS PD 4300A, 5.1.1.3: Guest Account
- DHS PD 4300A, 5.1.1.3: Initial Password
- DHS PD 4300A, 5.1.1.3: No Null Passwords
- DHS PD 4300A, 5.1.1.3 Password Storage
- DHS PD 4300A, 5.1.1.3 Privileged Accounts
- DHS PD 4300A, 5.2.c: Sharing Passwords
- Incident Response Training (IR-2)
- Incident Response Testing (IR-3)
- Incident Handling (IR-4)
- Incident Monitoring (IR-5)
- Incident Reporting (IR-6)
- Incident Response Assistance (IR-7)
- DHS PD 4300A, 3.14..c: Privacy Inc. Reporting
- DHS PD 4300A, 3.14.6.d: Privacy Inc. Reporting
- DHS PD 4300A, 3.15.g: CFO Incident Response
- DHS PD 4300A, 3.15.h: CFO Incident Reporting
- DHS PD 4300A, 4.9.b: SOC
- DHS PD 4300A, 4.9.1.a: Incident Response
- DHS PD 4300A, 4.9.1.b: Incident Response
- DHS PD 4300A, 4.9.1.c: HSDN Incidents
- DHS PD 4300A, 4.9.1.d: Minor Incidents
- DHS PD 4300A, 4.9.1.e: Incident Reporting
- DHS PD 4300A, 4.9.1.f: Incident Reporting
- DHS PD 4300A, 4.9.1.k: SOC/CSIRC
- DHS PD 4300A, 4.9.1.r: Incident testing

- DHS PD 4300A, 4.9.2.a: External law enforcement
- DHS PD 4300A, 4.9.2.b: LE/CI Incident Handling
- DHS PD 4300A, 5.4.4.e: Security ops
- Media Access (MP-2)
- Media Storage (MP-4)
- DHS PD 4300A, 4.3.1.a: Media
- DHS PD 4300A, 4.3.1.c: Removable Media
- Physical Access Authorizations (PE-2)
- Physical Access Control (PE-3)
- Visitor Control (PE-7)
- Delivery and Removal (PE-16)
- DHS PD 4300A, 4.2.1.c: Security Controls
- DHS PD 4300A, 4.2.1.d: Visitor Access
- DHS PD 4300A, 4.2.1.e: Physical Controls
- DHS PD 4300A, 4.2.2.a: Facility Protection
- Boundary Protection (SC-7)
- Protection of Information at Rest (SC-28)
- WITHDRAWN: Transmission Preparation Integrity (SC-33)
- DHS PD 4300A, 4.5.2.a: Fax Controls
- DHS PD 4300A, 4.5.3.b: Teleconference
- DHS PD 4300A, 5.4.3.i: Policy Enforcement Points
- DHS PD 4300A, 5.4.4.d: Quarterly Firewall Testing
- DHS PD 4300A, 5.4.4.f: Firewall Administration
- DHS PD 4300A, 5.4.4.g: Policy Enforcement Points (PEP)
- DHS PD 4300A, 5.4.4.h: Protocols and Services
- DHS PD 4300A, 5.4.5.a: Internet Connectivity
- DHS PD 4300A, 5.4.5.c: Mobile code

VULNERABILITY ASSESSMENT

MINIMUM REQUIRED TESTS FOR CFO DESIGNATED SYSTEMS:

CONFIGURE TESTING TOOLS TO VERIFY THAT:

- FIREWALLS, ROUTERS, AND NETWORK DEVICES WITHIN THE SYSTEM BOUNDARY ARE CONFIGURED IN ACCORDANCE WITH DHS GUIDELINES
- SYSTEM IS NOT VULNERABLE TO BUFFER OVERFLOW OR SIMILAR ATTACKS
- ALL RELEVANT APPLICATION, DATABASE, AND OPERATING SYSTEM SECURITY PATCHES HAVE BEEN APPROPRIATELY APPLIED IN ACCORDANCE WITH DHS GUIDELINES
- SYSTEM DEFAULT ACCOUNTS ARE RENAMED OR DELETED IF NOT NEEDED
- BLANK, GENERIC, AND ANONYMOUS PASSWORDS TO SERVICES SUCH AS FTP, TELNET, AND WEB SERVERS ARE NOT BEING USED
- INAPPROPRIATE ACCESS RIGHTS HAVE NOT BEEN GRANTED TO ACCOUNT PROFILES, ROLES, OR GROUPS
- AUDIT RECORDS ARE CONFIGURED APPROPRIATELY
- ACCESS TO AUDIT RECORDS AND TOOLS IS APPROPRIATELY RESTRICTED

ADDITIONAL RECOMMENDED TESTS FOR CFO-DESIGNATED SYSTEMS

- REVIEW OPEN PORTS TO IDENTIFY ANY UNNECESSARY NETWORK SERVICES
- REVIEW SCAN RESULTS FOR INDICATIONS OF UNAUTHORIZED AND/OR UNLICENSED SOFTWARE
- ENSURE THAT INTRUSION DETECTION MECHANISMS ARE APPROPRIATELY CONFIGURED AND IDENTIFIED NETWORK TRAFFIC ASSOCIATED WITH THE VULNERABILITY ASSESSMENT SCANS

DOCUMENTATION

ENSURE THAT THE FOLLOWING DOCUMENTS ARE COMPLETE, ACCURATE, AND CURRENT:

- DHS ARTIFACTS IN TAF:
  - SSP
  - RA
  - INTERCONNECTION SECURITY AGREEMENTS (ISA)

- Memorandums of Agreement (MOA) / Memorandums of Understanding (MOU)

- Documents to be managed by ISSO:
  - Security alerts and advisories, including date received and actions taken
  - Security incident/privacy incident reports: Copies of all security incident/privacy incident reports, including actions taken and date/time reported, as well as any follow-up or after action reports
  - Records of audit record review: including date of each review and person(s) performing review, as well as any suspicious activity identified and actions taken
  - Audit trails and activity logs
  - Physical access policies and procedures (if not in SSP)
- Documents to be monitored by ISSO:
  - List of user accounts: System generated list of users, including date created and date of last logon
  - List of transferred or separated employees/contractors, including date of separation and date of access removal (account disabled or removed)
  - User recertification results: Date of last validation of user and administrator access privileges, including person(s) performing the review and access changes
  - Access authorization forms: Access request and approval forms for users, system administrators, DBAs, and application developers/programmers
  - List of privileged user accounts: System generated list of system administrators, DBAs, and application developers/programmers, including date created and date of last logon
  - User, system administrator, DBA, and application developer/programmer access authorization forms: Access request and approval forms for users, system administrators, DBAs, and application developers/programmers
  - List of system software and utility users
  - List of application programmers
  - Tape and media control logs
  - Incident response training records, including dates of most recent initial or refresher incident response training for each individual with significant incident response roles and responsibilities
  - Access list for facility and data center: A list of all personnel granted physical access, including the date access was granted and the areas/facilities authorized for access
  - Physical access request and authorization forms (Examples and for specific users)
  - Emergency exit and re-entry procedures for the data center

2.3 CONFIGURATION MANAGEMENT

CONFIGURATION MANAGEMENT (CM) CONTROLS PROVIDE REASONABLE ASSURANCE THAT CHANGES TO INFORMATION SYSTEM RESOURCES ARE AUTHORIZED AND SYSTEMS ARE CONFIGURED AND SECURELY AND AS INTENDED, INCLUDING EFFECTIVE

- CONFIGURATION MANAGEMENT POLICIES, PLANS, AND PROCEDURES
- PROPER AUTHORIZATION, TESTING, APPROVAL, AND TRACKING OF ALL CONFIGURATION CHANGES
- ROUTINE MONITORING OF THE CONFIGURATION
- UPDATING SOFTWARE ON A TIMELY BASIS TO PROTECT AGAINST KNOWN VULNERABILITIES
- DOCUMENTATION AND APPROVAL OF EMERGENCY CHANGES TO THE CONFIGURATION

2.3.1 CM COMPLIANCE ACTIVITIES

Compliance Review
Conduct the following compliance review procedures in RTM: • Configuration Change Control (CM-3) • Monitoring Configuration Changes (CM-4) • Access Restrictions for Change (CM-5) • DHS PD 4300A, 4.4.1.a: PBX • DHS PD 4300A, 4.5.1.a: Telecomm Protection • DHS PD 4300A, 4.6.3.a: Wireless Security • DHS PD 4300A, 4.8.1.a: Workstations • DHS PD 4300A, 4.8.4.c: CM • DHS PD 4300A, 4.8.4.d Risk Mgmt • DHS PD 4300A, 4.1.b: Documentation • DHS PD 4300A, 5.4.3.l: CCB • DHS PD 4300A, 5.4.5.b: Firewalls and PEPs • DHS PD 4300A, 5.4.5.d Telnet • DHS PD 4300A, 5.4.5.e: FTP • Information System Documentation (SA-5)

- USER INSTALLED SOFTWARE (SA-7)
- DHS PD 4300A, 3.6.B LIFE-CYCLE DOCUMENTATION
- DHS PD 4300A, 4.8.03.B: PERSONAL EQUIPMENT
- FLAW REMEDIATION (SI-2)
- SECURITY ALERTS AND ADVISORIES AND DIRECTIVES (SI-5)
- DHS PD 4300A, 3.7.C: CM
- DHS PD 4300A, 5.4.2.A: NETWORK CONTINUOUS MONITORING
- DHS PD 4300A, 5.4.8.D: COMPLIANCE

VULNERABILITY ASSESSMENT

MINIMUM REQUIRED TESTS FOR CFO DESIGNATED SYSTEMS:

- ENSURE SOFTWARE IN USE IS CURRENTLY SUPPORTED BY VENDOR

CONFIGURE TESTING TOOLS TO VERIFY THAT:

- ALL APPROPRIATE APPLICATION, DATABASE, AND OPERATING SYSTEM PATCHES AND UPDATES ARE INSTALLED BASED ON THE

RESULTS OF THE VULNERABILITY ASSESSMENT SCANS, ENSURE THAT:

- CHANGE REQUEST AND APPROVAL FORMS ARE ON FILE FOR ANY CHANGES MADE TO SYSTEM HARDWARE AND SOFTWARE (E.G., SOFTWARE VERSION UPGRADES) SINCE THE SYSTEM WAS GRANTED ATO
- NECESSARY WAIVERS AND/OR EXCEPTIONS ARE MAINTAINED ON FILE FOR ANY DEVIATIONS FROM DHS CONFIGURATION GUIDELINES IDENTIFIED DURING THE VULNERABILITY ASSESSMENT SCAN

ADDITIONAL RECOMMENDED TESTS FOR CFO DESIGNATED SYSTEMS:

- NONE

DOCUMENTATION

ENSURE THAT THE FOLLOWING DOCUMENTS ARE COMPLETE, ACCURATE, AND CURRENT:

- DHS ARTIFACTS IN TAF:
  - SSP
  - CHANGE MANAGEMENT PLAN
- DOCUMENTS TO BE MANAGED BY ISSO:
  - CONFIGURATION BASELINE (AFTER HARDENING)

- Listing of all vendor supplied software
- System software documentation

- Documents to be Monitored by ISSO:
  - System/program change requests and approvals
  - Security alerts and advisories, including date received and actions taken
  - System/program change requests and approvals

2.4 CONTINGENCY PLANNING

CONTINGENCY PLANNING (CP) CONTROLS PROVIDE REASONABLE ASSURANCE THAT CONTINGENCY PLANNING (1) PROTECTS INFORMATION RESOURCES AND MINIMIZES THE RISK OF UNPLANNED INTERRUPTIONS AND (2) PROVIDES FOR RECOVERY OF CRITICAL OPERATIONS SHOULD INTERRUPTIONS OCCUR, INCLUDING EFFECTIVE:

- ASSESSMENT OF THE CRITICALITY AND SENSITIVITY OF COMPUTERIZED OPERATIONS AND IDENTIFICATION OF SUPPORTING RESOURCES,
- STEPS TAKEN TO PREVENT AND MINIMIZE POTENTIAL DAMAGE AND INTERRUPTION,
- COMPREHENSIVE CONTINGENCY PLAN, AND
- PERIODIC CONTINGENCY PLAN TESTING, WITH APPROPRIATE ADJUSTMENTS TO THE PLAN BASED ON TESTING RESULTS

.COMPLIANCE REVIEW

CONDUCT THE FOLLOWING COMPLIANCE REVIEW PROCEDURES IN RTM:

- CONTINGENCY PLAN TESTING (CP-4)
- ALTERNATE PROCESSING SITES (CP-7)
- TELECOMMUNICATIONS SERVICES (CP-8)
- DHS PD 4300A, 3.15.F CONTINGENCY PLANNING
- DHS PD 4300A, 4.11.C BACKUP PROCEDURES
- SECURITY CATEGORIZATION (RA-2)
- DHS PD 4300A, 3.15.D CFO CIA MINIMUM
- INFORMATION SYSTEM DOCUMENTATION (SA-5)

VULNERABILITY ASSESSMENT

MINIMUM REQUIRED TESTS FOR CFO DESIGNATED SYSTEMS:

- NONE

ADDITIONAL RECOMMENDED TESTS FOR CFO DESIGNATED SYSTEMS:

- NONE

DOCUMENTATION

Ensure that the following documents are complete, accurate, and current:

- DHS Artifacts in IACS:
  - Contingency Plan
  - Annual Contingency Plan Test Results
  - Annual Disaster Recovery Exercise Results (for high availability systems)
- Documents to be Managed by ISSO:
  - Backup and restoration test results
- Documents to be Monitored by ISSO:
  - None

2.5 SEGREGATION OF DUTIES

SEGREGATION OF DUTIES (SD) CONTROLS PROVIDE REASONABLE ASSURANCE THAT INCOMPATIBLE DUTIES ARE EFFECTIVELY SEGREGATED, INCLUDING EFFECTIVE

- SEGREGATION OF INCOMPATIBLE DUTIES AND RESPONSIBILITIES AND RELATED POLICIES, AND
- CONTROL OF PERSONNEL ACTIVITIES THROUGH FORMAL OPERATING PROCEDURES, SUPERVISION, AND REVIEW.

2.5.1 SD COMPLIANCE ACTIVITIES

COMPLIANCE REVIEW

CONDUCT THE FOLLOWING COMPLIANCE REVIEW PROCEDURES IN RTM:

- SEPARATION OF DUTIES (AC-5)
- DHS PD 4300A, 4.1.4.A SEPARATION OF DUTIES
- ACCESS AGREEMENTS (PS-6)

VULNERABILITY ASSESSMENT

MINIMUM REQUIRED TESTS FOR CFO DESIGNATED SYSTEMS:

CONFIGURE TESTING TOOLS TO VERIFY THAT:

- INAPPROPRIATE ACCESS RIGHTS HAVE NOT BEEN GRANTED TO ACCOUNT GROUPS, ROLES, OR PROFILES

ADDITIONAL RECOMMENDED TESTS FOR CFO DESIGNATED SYSTEMS:

- NONE

DOCUMENTATION

ENSURE THAT THE FOLLOWING DOCUMENTS ARE COMPLETE, ACCURATE, AND CURRENT:

- DHS ARTIFACTS IN TAF:
  - SSP
- DOCUMENTS TO BE MANAGED BY ISSO:
  - NONE
- DOCUMENTS TO BE MONITORED BY ISSO:
  - LIST OF USERS AND THEIR POSITIONS
  - COPIES OF ALL POSITION DESCRIPTIONS

U.S. CUSTOMS AND BORDER PROTECTION

ATTACHMENT X

SOCIAL MEDIA

HB 1400-05D

INFORMATION SYSTEMS SECURITY POLICIES

VERSION

7.0

NOVEMBER 16, 2017

THIS PAGE LEFT INTENTIONALLY BLANK

DOCUMENT CHANGE HISTORY

VERSION	DATE	DESCRIPTION
4.0	APRIL 30, 2013	STYLISTIC AND FORMATTING CHANGES THROUGHOUT THE DOCUMENT.
5.0	JUNE 17, 2014	NO CHANGE.
6.0	MARCH 3, 2016	NO CHANGE.
6.01	MAY 17, 2016	NO CHANGE.
6.02	SEPTEMBER 2016	NO CHANGE.
7.0	NOVEMBER 16 , 2017	NO CHANGE.

CONTENTS

1.0 INTRODUCTION 1

1.1 BACKGROUND 1

1.2 PURPOSE AND SCOPE 2

1.3 APPLICATION 2

2.0 USE OF SOCIAL MEDIA 3

2.1 OFFICIAL USE OF SOCIAL MEDIA 3

2.1.1 GOVERNANCE 3

2.1.2 PRIVACY ISSUES 3

2.1.3 STANDARDS OF CONDUCT 4

2.2 UNOFFICIAL OR PERSONAL USE OF SOCIAL MEDIA ON GOVERNMENT EQUIPMENT 5

2.3 UNOFFICIAL OR PERSONAL USE OF SOCIAL MEDIA ON NON-GOVERNMENT EQUIPMENT 5

3.0 RISKS AND ATTACK TECHNIQUES ASSOCIATED WITH SOCIAL MEDIA 6

3.1 COMMON RISKS OF CYBER ATTACKS 6

3.2 COMMON CYBER ATTACK TECHNIQUES 7

3.2.1 SPEAR PHISHING 7

3.2.2 SOCIAL ENGINEERING 7

3.2.3 WEB APPLICATION ATTACKS 8

4.0 BEST PRACTICES FOR SOCIAL MEDIA USE 9

4.1 PERSONAL USE OF SOCIAL MEDIA 9

4.2 NO CLASSIFIED INFORMATION 9

4.3 DO NOT COMMUNICATE DHS POLICIES 9

4.4 AVOID POSTING PERSONAL INFORMATION 9

4.5 USE PRIVACY AND SECURITY SETTINGS 9

4.6 BE WARY OF LOCATION-BASED SERVICES 9

4.7 USE PASSWORDS CAREFULLY 10

4.8 BE SUSPICIOUS ABOUT INSTALLING APPLICATIONS 10

4.9 BE WARY OF ALL LINKS 10

4.10 HAVE NO EXPECTATION OF PRIVACY 11

4.11 PROTECT PRIVACY 11

4.12 BE PROFESSIONAL 11

4.13 USE DISCLAIMERS 12

4.14 BE THE FIRST TO RESPOND TO YOUR OWN MISTAKES 12

4.15 BE YOURSELF 12

4.16 AVOID THE OFFENSIVE 12

4.17 DO NOT BREACH TRADEMARKS 12

4.18 RESPECT COPYRIGHT, FAIR USE, AND FINANCIAL DISCLOSURE LAWS..... 12

4.19 IF IN DOUBT, SEEK GUIDANCE. 12

5.0 UNOFFICIAL INTERNET POSTING GUIDELINES 13

GLOSSARY 15

1.0 INTRODUCTION

SOCIAL MEDIA SUCH AS FACEBOOK, TWITTER, AND WIKIPEDIA HAVE BECOME UBIQUITOUS IN OUR DAILY LIFE. IN 2010, NEARLY TWO-THIRDS OF ALL AMERICAN ADULT INTERNET USERS ENGAGED IN SOME FORM OF SOCIAL MEDIA ON A REGULAR BASIS.[1] DUE TO EXTENSIVE CASUAL INTERNET USE, IT COMES AS NO SURPRISE THAT FEDERAL EMPLOYEES AND CONTRACTORS MAY HAVE DIFFICULTY DECIDING WHAT CONSTITUTES ACCEPTABLE AND SECURITY-CONSCIOUS BEHAVIOR IN USING SOCIAL MEDIA..

EVEN AS GOVERNMENT ORGANIZATIONS CONSIDER HOW BEST TO LEVERAGE THE INTERACTIVITY ENABLED BY SOCIAL MEDIA, THEY MUST ALSO ENSURE A COMMON UNDERSTANDING OF HOW EMPLOYEES ARE EXPECTED TO USE THOSE MEDIA..

ISSUED UNDER THE AUTHORITY OF THE DEPARTMENT OF HOMELAND SECURITY (DHS) CHIEF INFORMATION OFFICER (CIO), THROUGH THE OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER (OCISO), THIS DOCUMENT EXPANDS ON EXISTING DEPARTMENT OF HOMELAND SECURITY (DHS) POLICY AS PROVIDED IN SECTION 3.16, "SOCIAL MEDIA," OF *DHS SENSITIVE SYSTEMS POLICY DIRECTIVE 4300A*, AND IN DHS MANAGEMENT DIRECTIVE (MD) 4400.1, "WEB (INTERNET, INTRANET, AND EXTRANET INFORMATION) AND INFORMATION SYSTEMS." THIS DOCUMENT IS APPLICABLE:

WHETHER OR NOT THE USE IS OFFICIAL (WORK-RELATED) OR UNOFFICIAL (PERSONAL)

WHETHER OR NOT THE USE OCCURS ON SANCTIONED "OFFICIAL" SOCIAL MEDIA SITES OR ON COMMERCIALLY MANAGED SITES

WHETHER OR NOT USE IS ACCOMPLISHED USING GOVERNMENT-ISSUED EQUIPMENT OR ON ELECTRONIC DEVICES OWNED BY THE EMPLOYEE OR OTHER THIRD-PARTY."

1.1 BACKGROUND

CYBERSECURITY TRENDS HAVE SHOWN INCREASING ATTACKS ON AND VIA SOCIAL MEDIA. DUE TO THE HIGH THREAT OF ***MALWARE*** INFILTRATION AND THE SENSITIVE NATURE OF THE INFORMATION MAINTAINED AT DHS, SOCIAL MEDIA HOST SITES ARE BLOCKED AT THE DEPARTMENT'S TRUSTED INTERNET CONNECTIONS (TIC)[2]. THE ASSISTANT SECRETARY, OFFICE OF PUBLIC AFFAIRS (OPA), AS WELL AS COMPONENT PUBLIC OR EXTERNAL AFFAIRS OFFICES, HOWEVER, DO PERMIT LIMITED SOCIAL MEDIA USE "BY EXCEPTION," THROUGH SANCTIONED "OFFICIAL" GOVERNMENT AND COMMERCIAL SOCIAL MEDIA SITES AND SOCIAL NETWORKING SERVICES. THESE LIMITED USES OF SOCIAL MEDIA MAKE INFORMATION AND SERVICES MORE WIDELY AVAILABLE TO ALLOW THE DEPARTMENT AND COMPONENT EMPLOYEES, AND THE PUBLIC TO:

- SUPPORT DEPARTMENT AND COMPONENT MISSIONS
- SHOWCASE THE DEPARTMENT'S WORK AND INTEGRATION
- REACH A WIDER AUDIENCE MORE EFFICIENTLY THROUGH THE USE OF SOCIAL MEDIA CAPABILITIES
- PROVIDE ADDITIONAL SOURCES THAT THE PUBLIC CAN USE TO OBTAIN SUPPLEMENTAL INFORMATION ABOUT THE DEPARTMENT'S ACTIVITIES
- PROVIDE OPPORTUNITIES FOR PARTICIPATION AND COLLABORATION ON DEPARTMENT ACTIVITIES

---

[1] KATHRYN ZICKUHR AND LEE RAINE, *WIKIPEDIA, PAST AND PRESENT*, PEW INTERNET & AMERICAN LIFE PROJECT, 13 JANUARY 2011. THIS 2010 SURVEY REPORTS THE FOLLOWING SOCIAL MEDIA USAGES AMONG AMERICAN ADULTS, AGE 18 AND OLDER: WIKIPEDIA (53%), INSTANT MESSAGING (47%), SOCIAL NETWORKING SITES (61%), VIDEO SHARING SITES LIKE YOUTUBE (66%).

[2] SECTION 3.16, *DHS SENSITIVE SYSTEMS POLICY DIRECTIVE 4300A*.

IN ADDITION, THE DEPARTMENT RECOGNIZES THAT INDIVIDUALS WHO ENGAGE IN UNOFFICIAL (PERSONAL) SOCIAL MEDIA MAY EASILY BECOME VICTIMS OF ***SOCIAL ENGINEERING*** OR OTHER FORMS OF CYBER-ATTACK. EMPLOYEES NEED GUIDANCE TO HELP MINIMIZE THE RISKS THEIR SOCIAL MEDIA USE POSES TO THE DEPARTMENT AND ITS MISSIONS.

1.2 PURPOSE AND SCOPE

THIS DOCUMENT PROVIDES INFORMATION SECURITY GUIDANCE REGARDING OFFICIAL (WORK-RELATED) AND UNOFFICIAL (PERSONAL) SOCIAL MEDIA USE WHETHER OCCURRING WITHIN OR OUTSIDE THE DEPARTMENT NETWORK.

1.3 APPLICATION

THIS DOCUMENT APPLIES TO ALL DHS EMPLOYEES AND CONTRACTORS, DESCRIBES THE GOVERNANCE OF SOCIAL MEDIA SITES ACROSS DHS, AND ADDRESSES THE USE AND ASSOCIATED RISKS OF SOCIAL MEDIA TECHNOLOGIES IN THREE SCENARIOS:

- REQUIRED WORK-RELATED USE
- UNOFFICIAL OR PERSONAL USE ON GOVERNMENT EQUIPMENT
- UNOFFICIAL OR PERSONAL USE ON NON-GOVERNMENT EQUIPMENT

THE TERM *EQUIPMENT* INCLUDES BOTH NON-PORTABLE DEVICES SUCH AS DESKTOP COMPUTERS AS WELL AS MOBILE DEVICES SUCH AS LAPTOP COMPUTERS AND PORTABLE ELECTRONIC DEVICES (FOR EXAMPLE BLACKBERRIES, SMARTPHONES, AND PDAS).

THIS DOCUMENT INCLUDES BEST PRACTICES AND GUIDANCE REGARDING ACCEPTABLE SOCIAL MEDIA USE. COMMONLY USED SOCIAL MEDIA TERMS ARE IN BOLD ITALICS THROUGHOUT THIS ATTACHMENT AND ARE DEFINED IN THE GLOSSARY.

2.0 USE OF SOCIAL MEDIA

2.1 OFFICIAL USE OF SOCIAL MEDIA

MANY FEDERAL DEPARTMENTS AND AGENCIES ARE REQUIRED TO POST GOVERNMENT INFORMATION TO SPECIFIC SITES. DHS.GOV IS THE OFFICIAL WEBSITE AND PRESENCE OF DHS, WHERE COMPONENT OFFICES OF PUBLIC OR EXTERNAL AFFAIRS PUBLISH MATERIALS ON DHS.GOV. IN ADDITION, SOME COMPONENTS MAINTAIN THEIR OWN WEBSITES, SUBJECT TO DEPARTMENTAL OVERSIGHT.

ENFORCEMENT OFFICERS, AS PART OF CHILD PORNOGRAPHY AND DRUG INTERDICTION TASK FORCES, ROUTINELY PERUSE EXTERNAL SOCIAL NETWORKS.

INSTRUCTIONS FOR USING DHS.GOV AND COMMERCIAL OR THIRD PARTY SOCIAL MEDIA ARE PROVIDED AT THE DHS WEB CENTER (SEE WWW.DHS.GOV/WEBCENTER).

AS A RESULT OF THESE TECHNOLOGICAL RELATIONSHIPS BETWEEN THE DEPARTMENT AND THE PUBLIC, IT IS IMPERATIVE THAT DHS ENGAGE THE PUBLIC IN A MANNER THAT COMPLIES WITH FEDERAL ACCESSIBILITY, PRIVACY, INFORMATION SECURITY, AND RECORDS LAWS.

2.1.1 GOVERNANCE

THE DHS OFFICE OF PUBLIC AFFAIRS (OPA) SERVES AS THE PRIMARY ACCOUNT HOLDER FOR ALL DHS AND COMPONENT SOCIAL MEDIA WEBSITES, APPROVES AND MANAGES ALL CONTENT POSTED, AND WHEN NECESSARY ACTS AS THE FINAL AUTHORITY ON COMMENT ACCEPTABILITY. OPA WILL ENSURE THAT POSTED CONTENT MEETS THE APPROPRIATE REQUIREMENTS FOR PUBLICLY AVAILABLE INFORMATION AND MATERIALS.

2.1.2 PRIVACY ISSUES

TO PROTECT PERSONALLY IDENTIFIABLE INFORMATION (PII) INTERNALLY AND WHEN ENGAGING THE PUBLIC, DHS EMPLOYEES MUST COMPLY WITH FEDERAL PRIVACY LAWS, OFFICE OF MANAGEMENT AND BUDGET (OMB) GUIDANCE, AND DHS PRIVACY POLICIES WHEN USING SOCIAL MEDIA IN AN OFFICIAL CAPACITY. THE PRIVACY OFFICE IS RESPONSIBLE FOR ENSURING THAT DHS USE OF SOCIAL MEDIA SUSTAINS AND DOES NOT ERODE PRIVACY PROTECTIONS CONCERNING THE USE, COLLECTION, AND DISCLOSURE OF ***PII.***

IT IS IMPERATIVE THAT THE DEPARTMENT BE TRANSPARENT ABOUT ITS USE OF SOCIAL MEDIA TO AVOID CONCERNS ABOUT UNAUTHORIZED SURVEILLANCE. THEREFORE, DHS MUST ENGAGE SOCIAL MEDIA WEBSITES IN A MANNER THAT PROTECTS PRIVACY AND RESPECTS USERS' INTENT. THE PUBLIC USER FULLY EXPECTS PRIVACY PROTECTIONS WHILE INTERACTING WITH THE DEPARTMENT. IN ORDER TO ADDRESS THESE AND OTHER CONCERNS, THE DHS PRIVACY OFFICE HAS SET FORTH SPECIFIC REQUIREMENTS FOR USING SOCIAL MEDIA IN A PRIVACY- SENSITIVE MANNER.

EACH SOCIAL MEDIA WEBSITE PROVIDES ITS OWN PRIVACY POLICY, AND WHILE USERS ARE TYPICALLY REQUIRED TO SUBMIT SOME PII DURING THE REGISTRATION PROCESS, THE DEPARTMENT WILL NEITHER SOLICIT NOR COLLECT SUCH PII. THE DEPARTMENT WILL EXAMINE THE SOCIAL MEDIA WEBSITE OR APPLICATION PRIVACY POLICY AND EVALUATE THE RISKS TO DETERMINE WHETHER OR NOT THE WEBSITE IS APPROPRIATE FOR THE DEPARTMENT'S USE. IF AN AGENCY POSTS A LINK THAT LEADS TO A SOCIAL MEDIA WEBSITE, THE AGENCY WILL PROVIDE AN ALERT TO THE VISITOR, EITHER A STATEMENT ADJACENT TO THE LINK OR A "POP-UP," EXPLAINING THAT VISITORS ARE BEING DIRECTED TO A NON-GOVERNMENT WEBSITE THAT MAY HAVE DIFFERENT PRIVACY POLICIES FROM THOSE OF THE AGENCY'S OFFICIAL WEBSITE.

THE DEPARTMENT WILL ONLY COLLECT THE MINIMUM INFORMATION NECESSARY FOR THE PROPER PERFORMANCE OF OFFICIAL FUNCTIONS. OFFICIAL DHS ACCOUNTS ON SOCIAL MEDIA WEBSITES WILL BE IDENTIFIED BY THE COMPONENT OR DEPARTMENT SEAL AND AN ANONYMOUS, EASILY IDENTIFIABLE ACCOUNT USER NAME INDICATING DHS PRESENCE, SUCH AS "DHS JOHN Q. EMPLOYEE."

AS PART OF THE DEPARTMENT'S PRIVACY COMPLIANCE PROCESS, THE DHS PRIVACY OFFICE HAS DEVELOPED TWO DEPARTMENT-WIDE PRIVACY IMPACT ASSESSMENTS (PIAS), BOTH FOUND AT WWW.DHS.GOV/PRIVACY, TO IDENTIFY AND MITIGATE PRIVACY RISKS:

"USE OF SOCIAL NETWORKING INTERACTIONS AND APPLICATIONS (COMMUNICATIONS/OUTREACH/PUBLIC DIALOGUE)," SEPTEMBER 16, 2010

"USE OF UNIDIRECTIONAL SOCIAL MEDIA APPLICATIONS," MARCH 8, 2011

THESE TWO PIAS AND THE DHS PRIVACY POLICIES, INCLUDING THOSE THAT ARE SOCIAL MEDIA SPECIFIC, GOVERN THE DEPARTMENT'S USE OF SOCIAL MEDIA FROM A PRIVACY STANDPOINT. THE DHS PRIVACY POLICY AS WELL AS PRIVACY POLICIES SPECIFIC TO SOCIAL MEDIA CAN BE FOUND AT WWW.DHS.GOV.

PIA DETERMINATION IS MADE ON A CASE BY CASE BASIS THROUGH THE SOCIAL MEDIA PRIVACY THRESHOLD ANALYSIS (PTA) PROCESS. APPROVED PIAS ARE PUBLISHED ON THE DEPARTMENT'S PRIVACY IMPACT ASSESSMENT WEB PAGE (SEE WWW.DHS.GOV/PRIVACY) UNLESS THEY ARE CLASSIFIED. DHS HAS ISSUED A PIA DETAILING THE PII TO WHICH THE DEPARTMENT MAY HAVE ACCESS BECAUSE OF ITS USE OF SOCIAL NETWORKING APPLICATIONS, HOW IT WILL USE THE INFORMATION, WHAT INFORMATION IS RETAINED AND SHARED, AND HOW INDIVIDUALS CAN GAIN ACCESS TO AND CORRECT THEIR INFORMATION.

DHS DOES NOT SOLICIT, COLLECT, OR DISSEMINATE PII FROM INDIVIDUALS WHO INTERACT WITH THE DEPARTMENT VIA SOCIAL MEDIA SITES. IF PII IS POSTED ON A SOCIAL MEDIA SITE, THE DEPARTMENT WILL ATTEMPT TO DELETE IT. IF THAT IS NOT POSSIBLE, THE DEPARTMENT WILL DISREGARD THE PII AND IT WILL NOT BE MAINTAINED IN AGENCY FILES. IT SHOULD BE NOTED, HOWEVER, THAT PII POSTED ON A SOCIAL MEDIA WEBSITE OR SENT TO THE DEPARTMENT IN CONNECTION WITH THE TRANSACTION OF PUBLIC BUSINESS MAY BECOME PART OF A FEDERAL RECORD AND WILL HAVE TO BE MAINTAINED IN ACCORDANCE WITH APPROPRIATE RECORDS RETENTION POLICIES.

IF A COMPONENT HAS AN OPERATIONAL NEED TO USE SOCIAL MEDIA OUTSIDE THE SCOPE OF THE REQUIREMENTS OUTLINED IN THE EXISTING PIAS, A SEPARATE PIA MUST BE COMPLETED AND APPROVED BY THE APPROPRIATE PRIVACY OFFICIAL. THE PIA SHOULD ADDRESS THE SPECIFIC PRIVACY CONCERNS THAT ARE UNIQUE TO THE COMPONENT.

2.1.3 STANDARDS OF CONDUCT

DHS EMPLOYEES AND CONTRACTORS ARE RESPONSIBLE FOR KNOWING AND FOLLOWING THE GUIDELINES IN DHS MANAGEMENT DIRECTIVE (MD) 4400.1, "WEB (INTERNET, INTRANET, AND EXTRANET INFORMATION) AND INFORMATION SYSTEMS" AND EXECUTIVE BRANCH CONDUCT GUIDELINES, SUCH AS "STANDARDS OF ETHICAL CONDUCT FOR EMPLOYEES OF THE EXECUTIVE BRANCH," WHEN USING SOCIAL MEDIA IN AN OFFICIAL CAPACITY. THESE STANDARDS COVER TOPICS OF PROHIBITED ACTIVITIES SUCH AS:

- ENGAGING IN VULGAR OR ABUSIVE LANGUAGE, PERSONAL ATTACKS OF ANY KIND, OR OFFENSIVE TERMS TARGETING INDIVIDUALS OR GROUPS
- ENDORSEMENT OF COMMERCIAL PRODUCTS, SERVICES, OR ENTITIES
- ENDORSEMENT OF POLITICAL PARTIES, CANDIDATES, OR GROUPS
- LOBBYING MEMBERS OF CONGRESS USING DHS OR ANY OTHER APPROPRIATED RESOURCE
- USE OF GOVERNMENT RESOURCES TO FOSTER COMMERCIAL INTERESTS OR INDIVIDUAL PROFIT

FEDERAL EMPLOYEES OFTEN INADVERTENTLY FAIL TO COMPLY WITH THE STRINGENT REQUIREMENTS OF THE HATCH ACT, WHICH GOVERNS POLITICAL SPEECH BY FEDERAL EMPLOYEES. RECENTLY, THE U.S. OFFICE OF SPECIAL COUNSEL (OSC) ISSUED GUIDANCE REGARDING THE APPLICABILITY OF THE HATCH ACT TO SOCIAL MEDIA ENGAGEMENT IN THE WORKPLACE BY FEDERAL EMPLOYEES. THE ACT'S RESTRICTIONS MAY DETERMINE WHETHER OR NOT FEDERAL EMPLOYEES ARE ALLOWED TO POST CONTENT THAT COULD BE INTERPRETED IN A POLITICAL LIGHT. EMPLOYEES SHOULD UNDERSTAND THE HATCH ACT AND SECTIONS 4 AND 5 OF THIS DOCUMENT BEFORE POSTING ON SOCIAL MEDIA SUCH AS BLOGS, FACEBOOK, AND TWITTER OR REVEALING PROFESSIONAL TITLES OR POLITICAL AFFILIATIONS.

2.2 UNOFFICIAL OR PERSONAL USE OF SOCIAL MEDIA ON GOVERNMENT EQUIPMENT

SOCIAL MEDIA IS AN ATTACK VECTOR ROUTINELY EXPLOITED BY CYBERCRIMINALS, WHOSE ACTIVITIES MAY EXPOSE THE DEPARTMENT TO UNACCEPTABLE RISK. ADDITIONALLY, SOCIAL NETWORK ACTIVITY CONSUMES BANDWIDTH AND CAN NEGATIVELY IMPACT EMPLOYEE PRODUCTIVITY. DHS PROHIBITS PERSONAL ACCESS TO SOCIAL MEDIA FROM GOVERNMENT EQUIPMENT UNLESS AN EXCEPTION TO POLICY HAS BEEN GRANTED.

ALTHOUGH DHS EMPLOYEES ARE AUTHORIZED LIMITED PERSONAL USE OF DHS OFFICE EQUIPMENT IN ACCORDANCE WITH DHS MANAGEMENT DIRECTIVE (MD) NO. 4600.1, "PERSONAL USE OF GOVERNMENT OFFICE EQUIPMENT," **SUCH AUTHORIZATION DOES NOT APPLY TO THE USE OF DHS EQUIPMENT FOR PERSONAL USE OF SOCIAL MEDIA**. THIS RESTRICTION ALSO APPLIES TO CONTRACTORS AND OTHER INDIVIDUALS USING DHS EQUIPMENT.

2.3 UNOFFICIAL OR PERSONAL USE OF SOCIAL MEDIA ON NON-GOVERNMENT EQUIPMENT

EMPLOYEE ACTIVITIES POTENTIALLY AFFECT DHS JOB PERFORMANCE, THE PERFORMANCE OF OTHERS, AND DHS BUSINESS INTERESTS. ANY INFORMATION POSTED ON THE INTERNET INCURS A LEVEL OF RISK, BECAUSE THAT INFORMATION IS EXPOSED INDEFINITELY WITH NO RELIABLE METHODS FOR DELETION OR RETRACTION. ADDITIONALLY, BECAUSE OF THE CONNECTED NATURE OF THE INTERNET, EVEN INFORMATION PRESUMED TO BE POSTED IN A VENUE WITH RESTRICTED ACCESS IS POTENTIALLY ACCESSIBLE TO ANYONE.

"UNOFFICIAL INTERNET POSTS [3]" RESULT WHEN DHS PERSONNEL EXPRESS DHS-RELATED THOUGHTS, IDEAS, KNOWLEDGE, EXPERIENCE, AND OPINIONS ON ANY INTERNET SITE, WHETHER OR NOT THE SITE IS DHS-CONTROLLED. UNOFFICIAL INTERNET POSTS ARE PERSONAL EXPRESSIONS DEVELOPED AND RELEASED BY AN EMPLOYEE OR CONTRACTOR THAT HAVE NOT BEEN INITIATED BY ANY OFFICIAL PART OF THE DHS ORGANIZATION OR REVIEWED THROUGH AN OFFICIAL DHS APPROVAL PROCESS. EMPLOYEES MUST REMEMBER THAT ANY INFORMATION ABOUT ANOTHER INDIVIDUAL IS ALMOST SURELY PROTECTED BY THE PRIVACY ACT AND SHOULD NOT BE SHARED.

SOCIAL NETWORKS ARE OF PARTICULAR CONCERN BECAUSE OF THE POTENTIAL FOR USERS TO DISSEMINATE PERSONAL INFORMATION ABOUT THEMSELVES AND OTHERS. UNLESS STRICT PRIVACY CONTROLS ARE APPLIED TO ONLINE PROFILES, THE INFORMATION POSTED IS VIEWABLE BY A WIDE RANGE OF STRANGERS. NORMALLY ADVERSARIES WOULD HAVE TO ENGAGE IN DETERMINED INFORMATION GATHERING IN ORDER TO COLLECT SENSITIVE INFORMATION, BUT SOCIAL NETWORKS CAN EASILY PROVIDE THEM AN OPPORTUNITY TO GATHER SENSITIVE INFORMATION WITH RELATIVE EASE. EVEN SEEMINGLY HARMLESS FACTS CAN BE COLLECTED AND USED BY ADVERSARIES TO ASSEMBLE PROFILES AND SELECT TARGETS. EVEN WITH PRIVACY CONTROLS IN PLACE, DHS EMPLOYEES AND CONTRACTORS SHOULD NOT POST ANY CONTENT THAT THEY WOULD NOT BE COMFORTABLE DISCLOSING TO THE PUBLIC.

[3] BASED ON US DHS, ALCOAST 548/08, COMDTNOTE 5700. SUBJ: SOCIAL MEDIA - UNOFFICIAL INTERNET POSTS

EMPLOYEES MUST REMEMBER THAT ANY INFORMATION THAT IS WORK-RELATED IS SENSITIVE AND CANNOT BE REPEATED OUTSIDE THE WORKPLACE WITHOUT APPROPRIATE APPROVAL. IN ADDITION, FURTHER LIMITS ARE IN PLACE IF YOU IDENTIFY YOURSELF, WHETHER DIRECTLY OR INDIRECTLY, AS A DHS EMPLOYEE.

CONSISTENT WITH THE RISKS DETAILED ABOVE, THE RECENT GUIDANCE ISSUED BY THE U.S. OFFICE OF SPECIAL COUNSEL (OSC) REGARDING SOCIAL MEDIA OUTSIDE THE WORKPLACE DOES NOT DIFFER SUBSTANTIALLY FROM GUIDANCE FOR THE WORKPLACE, ALTHOUGH MORE LATITUDE IS GIVEN FOR EMPLOYEES TO EXPRESS POLITICAL THOUGHTS AND CANDIDATE ADVOCACY AND SUPPORT ON THEIR PERSONAL WEBSITES. SEE SECTIONS 4 AND 5 OF THIS DOCUMENT FOR ADDITIONAL BEST PRACTICES AND GUIDELINES APPLICABLE TO SOCIAL MEDIA USE.

3.0 RISKS AND ATTACK TECHNIQUES ASSOCIATED WITH SOCIAL MEDIA

ADVERSARIES LOOK FOR OPPORTUNITIES TO EASILY TARGET PERSONS OF INTEREST ON THE INTERNET IN ORDER TO DEVELOP FOOTHOLDS FOR LONG-TERM SURVEILLANCE AND EXPLOITATION. SOCIAL MEDIA SITES ARE ATTRACTIVE TO HACKERS SINCE THE SAME TECHNOLOGIES THAT INVITE USER PARTICIPATION MAKE USER SYSTEMS EASY TO CORRUPT WITH ***MALWARE*** SUCH AS ***WORMS*** THAT CAN SHUT DOWN NETWORKS, ***SPYWARE,*** OR ***KEYSTROKE LOGGERS*** THAT CAN STEAL SENSITIVE DATA. FOR EXAMPLE, THE AVAILABILITY OF ***WIDGETS*** MAKES IT EASIER FOR SOCIAL NETWORKERS TO SHARE LINKS, INSERT PICTURES, ETC., BUT IT ALSO MAKES IT EASIER FOR AN ATTACKER TO SLIP IN MALICIOUS CODE OR TO LINK TO OFF-SITE CONTENT THAT CONTAINS ***MALWARE***.

3.1 COMMON RISKS OF CYBER ATTACKS

THE RISKS ASSOCIATED WITH SOCIAL NETWORKING FALL INTO A FEW BROAD CATEGORIES:

- HAVING THE SOCIAL NETWORKING ACCOUNT ITSELF HACKED
- USERS PICKING UP ***MALWARE*** THROUGH THE SOCIAL NETWORKING SITE
- HACKERS GAINING INFORMATION THROUGH A SOCIAL NETWORKING SITE THAT WILL ALLOW THE HACKER TO ATTACK THE ***ENTERPRISE NETWORK***
- ACCIDENTALLY RELEASING SENSITIVE INFORMATION
- IDENTITY THEFT

GOVERNMENT USE OF SOCIAL MEDIA ALSO POSES POTENTIAL PRIVACY RISKS. SOCIAL MEDIA USERS VOLUNTARILY PROVIDE PII IN THEIR USER PROFILES (EXAMPLES ARE HOMETOWN AND EMPLOYER), MAKING SUCH INFORMATION AVAILABLE TO OTHER REGISTERED USERS, INCLUDING DHS. THE AVAILABILITY OF THIS PII DOES NOT GIVE THE DEPARTMENT THE AUTHORITY OR RIGHT TO COLLECT, USE, OR DISCLOSE THAT INFORMATION FOR PURPOSES UNRELATED TO FOSTERING TRANSPARENCY AND OPEN GOVERNMENT ABSENT A SEPARATE AUTHORITY TO DO SO.

THE EMERGENCE OF ***LOCATION-BASED SERVICES (LBS)*** (GEO-LOCATION) POSES ADDITIONAL PRIVACY CONCERNS. RESEARCH UNDERTAKEN BY CARNEGIE MELLON UNIVERSITY IN 2009 AND 2010 FOUND THAT "CURRENTLY AVAILABLE LOCATION-SHARING SERVICES DO NOT, FOR THE MOST PART, DO A GOOD JOB OF INFORMING [USERS] ABOUT HOW THEIR LOCATION INFORMATION WILL BE USED OR PROVIDE USERS WITH EXPRESSIVE LOCATION PRIVACY CONTROLS AND PRIVACY-PROTECTIVE DEFAULT SETTINGS." FURTHERMORE, ALTHOUGH 222(F) OF THE COMMUNICATIONS ACT GENERALLY PROHIBITS WIRELESS CARRIERS FROM USING LOCATION-BASED INFORMATION FOR COMMERCIAL PURPOSES WITHOUT THE EXPRESS PRIOR CONSENT OF THE CONSUMER, THESE PROHIBITIONS DO NOT CURRENTLY APPLY TO LBS PROVIDERS EVEN THOUGH THEIR APPLICATIONS ARE BEING DOWNLOADED ON THE DEVICES OF WIRELESS CARRIERS. CONSUMERS MAY MISTAKENLY CONCLUDE THAT APPLICATION PROVIDERS ARE SUBJECT TO THE SAME PROHIBITIONS AS WIRELESS CARRIERS AND THAT NO ACTION BY CONSUMERS IS NECESSARY TO ENSURE THAT THEIR PRIVACY IS PROTECTED.[4]

3.2 COMMON CYBER ATTACK TECHNIQUES

ACCORDING TO THE *GUIDELINES FOR SECURE USE OF SOCIAL MEDIA BY FEDERAL DEPARTMENTS AND AGENCIES*, SOCIAL MEDIA TECHNOLOGIES SUCH AS *WIKIS, BLOGS*, AND *SOCIAL NETWORKS* ARE ESPECIALLY VULNERABLE TO THE FOLLOWING CYBER ATTACKS TECHNIQUES:[5]

- SPEAR PHISHING
- SOCIAL ENGINEERING
- WEB APPLICATION ATTACKS

3.2.1 SPEAR PHISHING

SPEAR PHISHING IS AN ATTACK TARGETING A SPECIFIC USER OR GROUP OF USERS, ATTEMPTING TO DECEIVE THE USER INTO PERFORMING AN ACTION THAT LAUNCHES AN ATTACK, SUCH AS OPENING A DOCUMENT OR CLICKING A LINK. SPEAR PHISHERS RELY ON KNOWING SOME PERSONAL PIECE OF INFORMATION ABOUT THEIR TARGET, SUCH AS AN EVENT, INTEREST, TRAVEL PLANS, OR CURRENT ISSUES. SOMETIMES THIS INFORMATION IS GATHERED BY HACKING INTO THE TARGETED NETWORK, BUT OFTEN IT IS EASIER TO LOOK UP THE TARGET ON A SOCIAL MEDIA NETWORK.

IN APRIL 2009, THE FEDERAL BUREAU OF INVESTIGATION RELEASED A HEADLINE ALERT SPECIFICALLY CITING SOCIAL NETWORKING SITES AS A MECHANISM FOR ATTACKERS TO GATHER INFORMATION ON THEIR TARGETS BY HARVESTING INFORMATION FROM PUBLICALLY ACCESSIBLE NETWORKS AND USING THE INFORMATION AS AN ATTACK VECTOR. SPEAR PHISHERS USE SOCIAL MEDIA AS AN ALTERNATIVE WAY TO SEND PHISHING MESSAGES, AS THE SOCIAL MEDIA PLATFORM BYPASSES TRADITIONAL EMAIL SECURITY CONTROLS. SECURITY TEAMS HAVE ALREADY OBSERVED MULTIPLE SOCIAL MEDIA WEBSITES USED AS A PROPAGATION MECHANISM TO TRICK USERS INTO OPENING A DOCUMENT OR CLICKING A LINK. DHS DAILY RECEIVES MANY SPECIFIC ATTACKS VIA EMAIL TARGETING SPECIFIC EMPLOYEES BY NAME AND POSITION.

3.2.2 SOCIAL ENGINEERING

THE SECOND CONCERN REGARDING SOCIAL MEDIA USE BY FEDERAL EMPLOYEES IS ***SOCIAL ENGINEERING***, WHICH RELIES ON EXPLOITING THE HUMAN TENDENCY TO TRUST. THE ATTACKER'S FIRST STEP IN ANY SOCIAL ENGINEERING ATTACK IS TO COLLECT INFORMATION ABOUT THE TARGET. SOCIAL NETWORKING WEBSITES CAN REVEAL MANY DETAILS OF PERSONAL INFORMATION, INCLUDING RESUMES, HOME ADDRESSES, PHONE NUMBERS, EMPLOYMENT INFORMATION, WORK LOCATIONS, FAMILY MEMBERS, EDUCATION, AND PHOTOS. SOCIAL MEDIA WEBSITES MAY SHARE MORE PERSONAL INFORMATION THAN USERS EXPECT, NEED, OR REALIZE.

FOR EXAMPLE, A STUDY BY THE UNIVERSITY OF VIRGINIA CITES THAT OUT OF THE TOP 150 FACEBOOK APPLICATIONS, ALL OF WHICH ARE EXTERNALLY HOSTED, OVER 90% NEEDED NOTHING MORE THAN PUBLICLY AVAILABLE INFORMATION FROM MEMBERS IN ORDER TO OPERATE. IN EVERY CASE, HOWEVER, USERS NEEDLESSLY GRANTED THE APPLICATIONS TOTAL ACCESS TO THEIR ACCOUNT AND THEREFORE FULL ACCESS TO ALL PERSONAL INFORMATION.

[4] *JOINT HEARING ON "THE COLLECTION AND USE OF LOCATION INFORMATION FOR COMMERCIAL PURPOSES", FEBRUARY 24, 2010.*

[5] *GUIDELINES FOR SECURE USE OF SOCIAL MEDIA BY FEDERAL DEPARTMENTS AND AGENCIES, VERSION 1.0, FEDERAL CIO COUNCIL, SEPTEMBER 2009*

WHEN DHS EMPLOYEES JOIN A SOCIAL MEDIA WEBSITE, THEY MAY IDENTIFY THEMSELVES AS DHS EMPLOYEES. THEIR SELF-IDENTIFICATION CREATES A DHS ***INTERNET FOOTPRINT*,** WHICH IS VALUABLE INFORMATION TO ADVERSARIES. AS MORE FEDERAL EMPLOYEES SELF-IDENTIFY ON SOCIAL MEDIA WEBSITES, THE FEDERAL FOOTPRINT ON SOCIAL NETWORKING WILL GROW, CREATING A TARGET-RICH ENVIRONMENT TO HELP ADVERSARIES TARGET SPECIFIC INDIVIDUALS TO LAUNCH VARIOUS SOCIAL ENGINEERING ATTACKS.

TO LEARN PERSONAL INFORMATION ABOUT AN INDIVIDUAL, AN ATTACKER CAN EXPRESS A COMMON INTEREST IN A TOPIC, AND BUILD A TRUST RELATIONSHIP WITH THE VICTIM. THIS POSITIONS THE ATTACKER TO INFLUENCE THE VICTIM'S FRIENDS AND CO-WORKERS OR EVEN TO COLLECT SUFFICIENT INFORMATION TO POSE AS THE VICTIM, PROVIDING AN EASY AVENUE FOR PENETRATING THE TRUST OF THE DEPARTMENT OR OF OTHER DHS PERSONNEL.

HIGH-PROFILE FEDERAL EMPLOYEES WITH GREATER NAME RECOGNITION CREATE AN EVEN LARGER FOOTPRINT., AND IS AN ESPECIALLY PRIME TARGET FOR A SOCIAL ENGINEER SEEKING TO EXPLOIT TRUST RELATIONSHIPS IN SOCIAL NETWORKS.

3.2.3 WEB APPLICATION ATTACKS

MALICIOUS CONTENT ON SOCIAL NETWORKING SITES IS EASY TO DISGUISE AS VALID CONTENT. DEVELOPERS OF USER-GENERATED GAMES AND APPLICATIONS ON SOME SITES HAVE THE OPTION OF GOING THROUGH AN APPROVAL PROCESS, BUT THE APPLICATION'S CODE IS NOT ALWAYS LOCKED IN THE STATE IN WHICH IT WAS SUBMITTED FOR APPROVAL. THIS CREATES A SITUATION IN WHICH APPARENTLY VETTED SOFTWARE CAN BE INJECTED WITH MALICIOUS CODE AT A LATER TIME.

FINALLY, WHILE A HIJACKED PERSONAL SOCIAL MEDIA ACCOUNT MAY BE ANNOYING AND PERSONALLY COSTLY OR EMBARRASSING, THE HIJACKED ACCOUNT OF A FEDERAL USER OR A HIJACKED FEDERAL ACCOUNT CAN HAVE MORE SERIOUS IMPLICATIONS. UNAUTHORIZED POSTS, TWEETS OR MESSAGES MAY BE SEEN BY THE PUBLIC AS OFFICIAL MESSAGES, OR MAY BE USED TO SPREAD MALWARE BY ENCOURAGING USERS TO CLICK LINKS OR DOWNLOAD MALWARE AND UNWANTED APPLICATIONS.

4.0 BEST PRACTICES FOR SOCIAL MEDIA USE

ONLINE ACTIVITIES OFTEN BLUR THE LINE BETWEEN INDIVIDUALS' PERSONAL AND PROFESSIONAL LIVES. REAL- WORLD SOCIAL AND BUSINESS RULES HAVE COUNTERPARTS IN DIGITAL ENVIRONMENTS. DHS EMPLOYEES OR CONTRACTORS, IN OR OUTSIDE OF THE WORKPLACE, MAY AFFECT THEIR JOB PERFORMANCE, THE PERFORMANCE OF OTHERS, OR DHS BUSINESS INTERESTS, SO THEY ARE A PROPER AUDIENCE FOR BEST PRACTICE GUIDANCE. THE FOLLOWING GUIDELINES ARE INTENDED TO ASSIST DHS EMPLOYEES AND CONTRACTORS IN PROTECTING THEIR PERSONAL INFORMATION AND REPUTATION WHILE INTERACTING ONLINE. THESE BEST PRACTICES ARE BASED ON GUIDELINES ESTABLISHED BY OTHER FEDERAL AND COMMERCIAL ORGANIZATIONS.

4.1 PERSONAL USE OF SOCIAL MEDIA

DO IT ONLY ON PERSONAL TIME USING YOUR PERSONAL COMPUTER AND E-MAIL ACCOUNT. YOU SHOULD NOT BE LOGGED ONTO EXTERNAL SOCIAL NETWORKING SITES WHILE AT WORK.

4.2 NO CLASSIFIED INFORMATION

DO NOT POST CLASSIFIED OR SENSITIVE INFORMATION. THIS CAN LEAD TO SIGNIFICANT ADVERSE ACTION AND PENALTIES. **DO NOT COMMUNICATE DHS POLICIES**

YOU SHOULD NOT ANSWER QUESTIONS OR MAKE STATEMENTS ABOUT OR ON BEHALF OF DHS ON A SOCIAL NETWORKING SITE WITHOUT EXPLICIT AUTHORIZATION FROM DHS OFFICE OF PUBLIC AFFAIRS, THE DHS OFFICE OF GENERAL COUNSEL, OR THEIR COMPONENT EQUIVALENT.

4.4 AVOID POSTING PERSONAL INFORMATION

LIMIT THE AMOUNT OF PERSONAL INFORMATION YOU WILLINGLY POST TO SOCIAL NETWORKS. AVOID POSTING PERSONAL INFORMATION LIKE YOUR HOME ADDRESS, PERSONAL PHONE NUMBERS, OR DETAILS ABOUT YOUR SCHEDULE OR ROUTINE. THIS TYPE OF INFORMATION GIVES CYBERCRIMINALS THE BASELINE THEY NEED FOR MORE TARGETED ACTIVITIES. ASSUME THAT ANYTHING YOU MIGHT POST TO A SOCIAL NETWORK CAN BE SEEN BY ANYONE AND ACT ACCORDINGLY. ALSO, BE WARY OF THE TYPE OF INFORMATION — INCLUDING PHOTOGRAPHS — THAT YOU POST ABOUT YOUR FRIENDS AND FAMILY, SINCE THAT INFORMATION CAN PUT THEM AT RISK.

4.5 USE PRIVACY AND SECURITY SETTINGS

WHEN ACCESSING SOCIAL NETWORKING SITES, YOU CAN LIMIT DISCLOSURE BY USING THE PRIVACY SETTINGS THAT ARE AVAILABLE. THE DEFAULT SETTINGS FOR SOME SITES MAY ALLOW ANYONE TO SEE YOUR PROFILE. YOU CAN CUSTOMIZE YOUR SETTINGS TO RESTRICT ACCESS TO ONLY CERTAIN PEOPLE. ALSO BE AWARE OF ANY CHANGES TO THE SITE'S PRIVACY/SECURITY OPTIONS. FOR EXAMPLE, IN 2009 FACEBOOK MADE MAJOR CHANGES TO USER PRIVACY SETTINGS. SOME OF THE NEW SETTINGS REPLACED PREVIOUS SETTINGS AND RESET THEM TO BE "VIEWABLE BY EVERYONE." USERS SHOULD MONITOR THE PRIVACY POLICIES FOR SOCIAL NETWORKING SITES AS THEY CHANGE OFTEN AND WITHOUT WARNING. REMEMBER THOUGH, THERE IS A RISK THAT EVEN PRIVATE INFORMATION CAN BE EXPOSED, SO DO NOT POST ANYTHING THAT YOU WOULD NOT WANT THE PUBLIC TO SEE.

4.6 BE WARY OF LOCATION-BASED SERVICES

BE AWARE OF PRIVACY AND SECURITY ISSUES WHEN USING LOCATION- BASED SERVICES (LBS). LOCATION- BASED SERVICES OFFER MANY CONVENIENCES SUCH AS KEEPING TRACK OF FAMILY AND FRIENDS, GETTING DIRECTIONS, FINDING RESTAURANTS, AND ASSISTING IN LAW ENFORCEMENT. BUT LBS MAY MAKE INFORMATION ABOUT YOUR LOCATION MAY BE ACCESSIBLE TO UNINTENDED RECIPIENTS. EMPLOYEES SHOULD UNDERSTAND THAT USE OF LBS INTRODUCES SIGNIFICANT PRIVACY AND PERSONAL SECURITY RISKS WITH THEIR USE. THE MOST COMMON EXAMPLE IS USING A LOCATION CHECK-IN SERVICE (FOR EXAMPLE, FOURSQUARE). IF YOU CHECK IN FROM YOUR COUCH AT HOME, THE PRECISE GLOBAL POSITIONING SYSTEM (GPS) COORDINATES OF YOUR COUCH ARE PUBLISHED. IF YOU LATER CHECK IN FROM YOUR OFFICE, IT CAN BE SEEN THAT OU ARE NO LONGER AT YOUR HOME, WHICH IS NOW AN EXCELLENT TARGET, AND YOUR OWN PERSONAL SECURITY CAN BE COMPROMISED.

YOU SHOULD ALSO BE AWARE THAT THIS INFORMATION MAY LEAK UNINTENTIONALLY. FOR EXAMPLE, SMART PHONES CAN ATTACH GPS COORDINATES TO PICTURES YOU TAKE. POSTS MADE TO SOCIAL MEDIA SITES SUCH AS FACEBOOK OR TWITTER MAY ALSO CONTAIN THIS DETAILED GEO-LOCATION DATA THAT COULD, AGAIN, COMPROMISE YOUR PERSONAL SECURITY AND POSSIBLY YOUR WORKPLACE SECURITY. THE LOCATION ATTACHED TO THE PICTURE MAY BE METADATA THAT IS UPLOADED WITHOUT YOUR KNOWLEDGE.

BE SURE TO EXAMINE YOUR PHONE'S PRIVACY, SECURITY, AND LOCATION SETTINGS TO ENSURE THAT GPS COORDINATES ARE NOT AUTOMATICALLY ASSOCIATED WITH LBS SERVICES. BE SURE NEVER TO CHECK IN FROM SENSITIVE LOCATIONS AND AVOID ESTABLISHING PATTERNS WHERE POSSIBLE.

4.7 USE PASSWORDS CAREFULLY

PROTECT YOUR ACCOUNT WITH PASSWORDS THAT CANNOT BE GUESSED EASILY. INSTEAD OF YOUR DOG'S NAME, THE WORD "PASSWORD" PLUS A DIGIT, OR YOUR FAVORITE SPORTS TEAM NAME, PASSWORDS SHOULD INCLUDE A COMBINATION OF UPPER AND LOWERCASE LETTERS, NUMBERS, AND SPECIAL CHARACTERS. EVEN SUCH STRONGLY CONSTRUCTED PASSWORDS ARE VULNERABLE TO KEYSTROKE LOGGERS AND PASSWORD CRACKING TOOLS. IN THE FINAL ANALYSIS, PASSWORDS DO LITTLE TO DETER A DETERMINED ATTACKER.

4.8 BE SUSPICIOUS ABOUT INSTALLING APPLICATIONS

APPLICATIONS FROM SOCIAL MEDIA SITES ARE VERY OFTEN GIVEN COMPLETE ACCESS TO YOUR ACCOUNT—NOT JUST TO WHAT IS NECESSARY FOR THE APPLICATION TO RUN. "QUIZZES" ARE ALSO PROBLEMATIC. FOR EXAMPLE, FACEBOOK USERS TAKING QUIZZES CAN REVEAL FAR MORE PERSONAL INFORMATION TO THE APPLICATIONS THAN THEY REALIZE. THIS IS MOSTLY DUE TO THE FACT THAT FACEBOOK'S DEFAULT PRIVACY SETTINGS ALLOW ACCESS TO ALL YOUR PROFILE INFORMATION WHETHER OR NOT YOUR PROFILE IS SET TO "PRIVATE." THE AMERICAN CIVIL LIBERTIES UNION (ACLU) REPORTS THAT EVEN IF YOU DO NOT TAKE QUIZZES YOURSELF, YOUR PROFILE INFORMATION IS REVEALED WHEN ONE OF YOUR FRIENDS TAKES A QUIZ. ALMOST EVERYTHING ON YOUR PROFILE, EVEN IF YOU USE PRIVACY SETTINGS TO LIMIT ACCESS, IS AVAILABLE TO THE QUIZ.[6]

4.9 BE WARY OF ALL LINKS

VIGILANCE IS THE BEST DEFENSE AGAINST PHISHING. PHISHING SCAMS CAN ARRIVE IN E-MAILS THAT LOOK AS THOUGH THEY COME FROM REAL COMPANIES OR TRUSTED INDIVIDUALS. FOR EXAMPLE, YOU MAY RECEIVE AN E-MAIL MESSAGE ANNOUNCING THAT YOUR BANK ACCOUNT WILL BE CLOSED UNLESS YOU CONFIRM YOUR PERSONAL IDENTIFICATION NUMBER, OR THAT YOU NEED TO PROVIDE YOUR CREDIT CARD INFORMATION TO CONFIRM AN ORDER, OR REQUESTING VERIFICATION OF YOUR SOCIAL SECURITY NUMBER FOR BILLING PURPOSES. LEGITIMATE COMPANIES DO NOT ASK FOR YOUR ACCOUNT OR PERSONAL INFORMATION VIA E-MAIL. TO FIND OUT WHETHER THE MESSAGE IS LEGITIMATE, CONTACT THE COMPANY DIRECTLY BY TELEPHONE OR LETTER USING CONTACT INFORMATION FROM A TRUSTED SOURCE, SUCH AS YOUR ACCOUNT STATEMENTS.

NEVER REPLY TO SUSPECT EMAILS OR CLICK ON ANY LINKS THEY CONTAIN. THIS COULD EXPOSE YOU TO CLICKJACKING, WHERE A WEB PAGE WILL TRICK YOU INTO PERFORMING UNDESIRED ACTIONS BY CLICKING ON CONCEALED BUTTONS OR LINKS THAT ARE ON A WEB PAGE HIDDEN BY THE VISIBLE ONE. FOR EXAMPLE, THE PAGE MAY LIST WHAT APPEARS TO BE A DHS URL (OR WEB PAGE ADDRESS, SUCH AS WWW.DHS.GOV), WHICH IN FACT HIDES THE LINK TO A WEB SITE SET UP BY A CYBERCRIMINAL. TO FIND OUT WHETHER THE MESSAGE IS LEGITIMATE, CONTACT THE SENDING COMPANY DIRECTLY BY TELEPHONE OR LETTER USING DATA FROM A TRUSTED SOURCE, SUCH AS YOUR ACCOUNT STATEMENTS OR THE BACK OF YOUR CREDIT/DEBIT CARD. AND INSTEAD OF SIMPLY CLICKING ON AN EMBEDDED LINK, MANUALLY TYPE THE URL INTO THE NAVIGATION BAR OF YOUR WEB BROWSER TO AVOID CLICKJACKING.

PHISHING ATTEMPTS CAN ALSO COME IN TWEETS (SEE TWITTER), FACEBOOK WALL POSTINGS, VIDEOS, OR PICTURES. FOR EXAMPLE, A FRIEND SENDING A LINK TO A FUNNY VIDEO MIGHT HAVE HAD HIS/HER ACCOUNT COMPROMISED. GET INTO THE HABIT OF NOT CLICKING ON HYPERLINKS, ESPECIALLY THOSE FOR VIDEOS OR NEWS-RELATED EVENTS. IN MANY CASES, THESE ARE LINKED TO PHISHING AND SOCIAL ENGINEERING ATTACKS

[6] S. PEREZ, "WHAT FACEBOOK QUIZZES KNOW ABOUT YOU," READWRITEWEB, AUGUST 27, 2009 7:29 AM.

4.10 HAVE NO EXPECTATION OF PRIVACY

ASSUME THAT YOUR THOUGHTS ARE IN THE PUBLIC DOMAIN. REMEMBER THAT SOCIAL NETWORKING SITES ARE GENERALLY PUBLIC AND PERMANENT, EVEN IF YOU DELETE THE INFORMATION YOU POSTED. YOU SHOULD UNDERSTAND THE SECURITY AND PRIVACY FEATURES AVAILABLE FOR THE SOCIAL NETWORKING SITES YOU USE, AND EXERCISE DISCRETION AND COMMON SENSE. MOST SOCIAL NETWORKS OFFER SETTINGS TO KEEP PROFILES PRIVATE AND RESTRICT ACCESS TO YOUR PHOTOGRAPHS OR OTHER PERSONALLY IDENTIFIABLE DETAILS; HOWEVER, OPTING FOR PRIVACY DOES NOT GUARANTEE THAT OTHERS WILL NOT SEE YOUR CONTENT. CONTENT CAN BE FORWARDED OR HACKED. FACEBOOK HAS FOUND ITSELF AT THE CENTER OF PRIVACY BREAKDOWN CONTROVERSIES NUMEROUS TIMES, AND CONFUSING TWITTER INTERFACES HAVE RESULTED IN PRIVATE MESSAGES BEING INADVERTENTLY POSTED TO PUBLIC FEEDS. HACKERS CAN FORCE ACCESS, AND FRIENDS CAN FORWARD YOUR CONTENT TO OTHERS. IN SHORT, DO NOT POST ANYTHING THAT YOU WOULD NOT WANT THE PUBLIC TO SEE.

4.11 PROTECT PRIVACY

YOU SHOULD NOT SHARE PERSONAL OR CONTACT INFORMATION ABOUT YOUR FAMILY, FRIENDS, CO-WORKERS, CLIENTS, OR BUSINESSES WITHOUT THAT INDIVIDUAL'S EXPLICIT CONSENT. YOU ALSO SHOULD NOT POST OR TAG PICTURES OF FAMILY, FRIENDS, CO-WORKERS, CLIENTS, OR BUSINESS WITHOUT THEIR CONSENT. RESPECT THE PRIVACY OF OTHERS AT ALL TIMES. YOU SHOULD ALWAYS PROTECT SENSITIVE INFORMATION SUCH AS PII.

4.12 BE PROFESSIONAL

IF YOU IDENTIFY YOURSELF AS A DHS EMPLOYEE OR HAVE A PUBLIC-FACING POSITION SO THAT YOUR DHS ASSOCIATION IS KNOWN TO THE GENERAL PUBLIC, ENSURE THAT YOUR PROFILE AND RELATED CONTENT ARE CONSISTENT WITH HOW YOU WISH TO PRESENT YOURSELF AS A DHS PROFESSIONAL, EVEN IF THE INFORMATION IS OF A PERSONAL AND UNOFFICIAL NATURE. ENSURE THAT ALL YOUR POSTS AND INTERACTIONS ARE CONSISTENT WITH THE PUBLIC TRUST ASSOCIATED WITH YOUR POSITION, AND CONFORM TO EXISTING STANDARDS SUCH AS "STANDARDS OF ETHICAL CONDUCT FOR EMPLOYEES OF THE EXECUTIVE BRANCH."

IF YOU ESTABLISH ONLINE PROFILES, YOU MAY PROVIDE YOUR DHS TITLE AND CONTACT INFORMATION. YOU MAY ALSO INDICATE THAT DHS IS YOUR EMPLOYER, AND YOU MAY DESCRIBE YOUR PAST AND PRESENT JOB RESPONSIBILITIES (AS YOU WOULD ON YOUR RESUME) IF YOU DO NOT DISCLOSE ANY DHS SENSITIVE INFORMATION OR THE PERSONAL INFORMATION OF OTHERS.

4.13 USE DISCLAIMERS

BE AWARE OF YOUR DHS ASSOCIATION IN ONLINE SOCIAL NETWORKS. IF YOUR PROFILE REVEALS YOUR EMPLOYMENT RELATIONSHIP WITH DHS, YOU SHOULD INCLUDE A DISCLAIMER STATING THAT YOUR ACTIVITY AND POSTS REPRESENT YOUR PERSONAL OPINIONS AND DO NOT REPRESENT THOSE OF DHS. AN EXAMPLE OF AN APPROPRIATE DISCLAIMER IS "THE POSTINGS ON THIS SITE ARE MY OWN AND DO NOT REPRESENT THE POSITIONS, STRATEGIES, OR OPINIONS OF THE DEPARTMENT OF HOMELAND SECURITY."

4.14 BE THE FIRST TO RESPOND TO YOUR OWN MISTAKES

IF YOU MAKE AN ERROR, BE UP FRONT ABOUT YOUR MISTAKE AND CORRECT IT QUICKLY. IN A BLOG, IF YOU CHOOSE TO MODIFY AN EARLIER POST, MAKE IT CLEAR THAT YOU HAVE DONE SO.

4.15 BE YOURSELF

DO NOT FORGE OR OTHERWISE MANIPULATE IDENTITIES IN YOUR POSTS IN AN ATTEMPT TO DISGUISE, IMPERSONATE, OR OTHERWISE MISREPRESENT YOUR IDENTITY OR AFFILIATION WITH ANY OTHER PERSON OR ENTITY.

4.16 AVOID THE OFFENSIVE

DO NOT POST ANY DEFAMATORY, LIBELOUS, VULGAR, OBSCENE, ABUSIVE, PROFANE, THREATENING, RACIALLY AND ETHNICALLY HATEFUL, OR OTHERWISE OFFENSIVE OR ILLEGAL INFORMATION OR MATERIAL.

4.17 DO NOT BREACH TRADEMARKS

DO NOT USE ANY WORD, LOGO, OR OTHER MARK THAT WOULD INFRINGE UPON THE TRADEMARK, SERVICE MARK, CERTIFICATION MARK, OR OTHER INTELLECTUAL PROPERTY RIGHTS OF THE OWNERS OF SUCH MARKS WITHOUT THE PERMISSION OF SUCH OWNERS.

4.18 RESPECT COPYRIGHT, FAIR USE, AND FINANCIAL DISCLOSURE LAWS.

DO NOT POST ANY INFORMATION OR OTHER MATERIAL PROTECTED BY COPYRIGHT WITHOUT THE PERMISSION OF THE COPYRIGHT OWNER. ALSO, CONSIDER USING A CREATIVE COMMONS LICENSE TO PROTECT YOUR OWN WORK. CREATIVE COMMONS OFFERS A FLEXIBLE COPYRIGHT MODEL THROUGH A COLLECTION OF FREE COPYRIGHT LICENSES WRITTEN IN PLAIN LANGUAGE. CREATORS CAN SELECT SEVERAL OF THESE LICENSES TO COMMUNICATE WHICH RIGHTS THEY RESERVE, AND WHICH THEY WAIVE, WHEN THEIR INTELLECTUAL PROPERTY IS USED BY OTHERS. WIKIPEDIA IS ONE OF THE MOST NOTABLE WEB-BASED PROJECTS USING A CREATIVE COMMONS LICENSE. SEE WWW.CREATIVECOMMONS.ORG FOR ADDITIONAL DETAILS.

4.19 IF IN DOUBT, SEEK GUIDANCE.

SEEK GUIDANCE FROM THE DHS OFFICE OF PUBLIC AFFAIRS OR THE DHS OFFICE OF GENERAL COUNSEL, OR COMPONENT EQUIVALENT, PRIOR TO SHARING PUBLICLY ANY PERSONAL OPINIONS OR STATEMENTS BASED ON YOUR ROLE WITHIN DHS. THOSE WITH LEADERSHIP RESPONSIBILITIES, BY VIRTUE OF THEIR POSITION, ESPECIALLY MUST UNDERSTAND THAT PERSONAL THOUGHTS THEY PUBLISH, EVEN IN CLEARLY PERSONAL VENUES, INADVERTENTLY MAY BE INTERPRETED AS EXPRESSIONS OF OFFICIAL DHS POSITIONS. THEY SHOULD ASSUME THAT THEIR CO-WORKERS, EMPLOYEES, AND THOSE OUTSIDE OF DHS WILL READ WHAT THEY HAVE WRITTEN.

5.0 UNOFFICIAL INTERNET POSTING GUIDELINES[7]

DEPARTMENT OF HOMELAND SECURITY (DHS) PERSONNEL WHO POST CONTENT ABOUT DHS ON THE INTERNET ARE RESPONSIBLE FOR ENSURING THAT ANY INFORMATION DISCLOSED (INCLUDING PERSONAL COMMENTS) IS ACCURATE AND APPROPRIATE. DHS PERSONNEL SHOULD KEEP IN MIND HOW THEIR POSTS WILL REFLECT UPON THEMSELVES AND THEIR ORGANIZATION, AND ALSO BE AWARE THAT SOME INDIVIDUALS AND GROUPS USE PUBLIC NETWORKING FORUMS TO GAIN INFORMATION THAT WILL HELP THEM ADVANCE THEIR OWN CAUSES OR AGENDAS AT THE EXPENSE OF OTHERS. DHS PERSONNEL WHO ENGAGE IN UNOFFICIAL POSTING ON THE INTERNET SHOULD OBSERVE THE FOLLOWING GUIDELINES:

(1) YOU MAY NOT RELEASE DHS E-MAIL ADDRESSES, TELEPHONE NUMBERS, OR FAX NUMBERS NOT ALREADY PUBLICLY RELEASED. YOU MAY NOT RELEASE THE CONTENT MANAGER'S OR CONTENT PROVIDER'S WORK CONTACT INFORMATION.

YOU MAY NOT POST OR DISCLOSE THE EXISTENCE OF INTERNAL DHS DOCUMENTS OR INFORMATION THAT DHS HAS NOT OFFICIALLY RELEASED TO THE PUBLIC. THIS POLICY APPLIES NO MATTER YOU OBTAINED THE INFORMATION. EXAMPLES INCLUDE, BUT ARE NOT LIMITED TO, THE FOLLOWING: MEMOS, E-MAILS, MEETING NOTES, ARTICLES FOR PUBLICATIONS, WHITE PAPERS, PUBLIC AFFAIRS GUIDANCE, AND ALL PRE-DECISIONAL MATERIALS. YOU MUST NOT RELEASE ANY FOR OFFICIAL USE ONLY (FOUO) INFORMATION OR PII IN UNOFFICIAL INTERNET POSTS.

YOU, AS A DHS EMPLOYEE OR CONTRACTOR, ARE ALWAYS RESPONSIBLE FOR ADHERING TO DHS POLICIES CONCERNING INFORMATION SECURITY, PHYSICAL SECURITY, AND TO THE PRIVACY ACT IN ALL FORMS OF COMMUNICATION. UNAUTHORIZED DISCLOSURE OF PROTECTED INFORMATION, INCLUDING SENSITIVE BUT UNCLASSIFIED (SBU) INFORMATION MAY RESULT IN DISCIPLINARY ACTION.

YOU MAY NOT RELEASING INFORMATION ABOUT OR PERTAINING TO ANOTHER DHS EMPLOYEE. RELEASE OF CLASSIFIED, OPERATIONAL, PROPRIETARY, LAW ENFORCEMENT SENSITIVE, OR INVESTIGATORY INFORMATION IS NOT AUTHORIZED.

ANY PHOTO, VIDEO, OR SOUND RECORDING MADE BY DHS PERSONNEL OF AN OFFICIAL DHS IS CONSIDERED OFFICIAL DHS MEDIA. NEWSWORTHY ITEMS SHOULD BE RELEASED OFFICIALLY TO NEWS ORGANIZATIONS AND OTHER MEDIA WITH THE KNOWLEDGE AND APPROVAL OF OPA OR THE COMPONENT OFFICE OF PUBLIC OR EXTERNAL AFFAIRS BEFORE BEING POSTING UNOFFICIALLY.

DHS-RELATED MEDIA MADE BY DHS PERSONNEL WHILE THEY ARE IN A NON-WORKING STATUS IN PUBLIC AREAS, (E.G., PHOTO OF A U.S. COAST GUARD CUTTER TAKEN FROM A PUBLIC PIER WHILE ON LIBERTY) IS CONSIDERED PRIVATE IMAGERY AND IS NOT SUBJECT TO THESE GUIDELINES.

USE OF OFFICIAL OR PROTECTED DHS STATEMENTS OR SYMBOLS (FOR EXAMPLE, THE DHS LOGO) MUST BE APPROVED OPA. THIS PREVENTS THE IMPRESSION OF OFFICIAL OR IMPLIED ENDORSEMENTS.

YOU MAY NOT RELEASE, INTENTIONALLY OR UNINTENTIONALLY, LOCATION-BASED (GEOSPATIAL) INFORMATION RELATED TO A DHS MISSION. THIS PROHIBITION INCLUDES, FOR EXAMPLE, DISCLOSING THE LOCATION OF THE EMPLOYEE AND/OR DHS ASSETS AT A PARTICULAR POINT IN TIME. ***AUTO- TWEETING,*** GEOSPATIAL COORDINATES WHILE DRIVING, OR REPORTING VIA A LOCATION-BASED SOCIAL MEDIA TOOL SUCH AS ***FOURSQUARE*** ARE EXAMPLES OF VIOLATIONS OF THIS GUIDELINE.

[7] BASED ON US DHS, ALCOAST 548/08, COMDTNOTE 5700. SUBJ: SOCIAL MEDIA - UNOFFICIAL INTERNET POSTS.

AS WITH OTHER FORUMS OF PERSONAL PUBLIC ENGAGEMENT, DHS PERSONNEL SHALL AVOID OFF-DUTY BEHAVIOR THAT NEGATIVELY IMPACTS OR CONFLICTS WITH THEIR ABILITY TO EXECUTE THEIR DUTIES FOR DHS, SUCH AS THE PROHIBITED PERSONAL CONDUCT DESCRIBED IN STANDARDS OF ETHICAL CONDUCT FOR EMPLOYEES OF THE EXECUTIVE BRANCH.

GLOSSARY

TERMS COMMONLY USED IN RELATION TO SOCIAL MEDIA ARE DEFINED BELOW.

BLOG	AN ABBREVIATION OF "WEBLOG." A BLOG IS A WEB-BASED FORUM WHERE INDIVIDUAL CONTENT PROVIDERS CONTRIBUTE REGULAR ENTRIES OR "POSTS" IN THE FORM OF COMMENTARY, DESCRIPTIONS OF EVENTS, OR OTHER MATERIALS ON THE WEBSITE. VISITORS TO THE BLOG MAY ADD THEIR OWN COMMENTS TO POSTS. BLOGS MAY BE "MODERATED" WITH THE BLOG OWNER OVERSEEING REMOVAL OF ANY OBJECTIONABLE MATERIAL, OR THEY MAY BE "UNMODERATED," IN WHICH CASE THERE IS NO CONTROL OVER THE POSTED MATERIAL.
CLICKJACKING	A MALICIOUS TECHNIQUE OF TRICKING A USER INTO REVEALING CONFIDENTIAL INFORMATION OR OF TAKING CONTROL OF THEIR COMPUTER WHEN THEY CLICK LINKS ON SEEMINGLY HARMLESS WEB PAGES. ON A CLICKJACKED PAGE, THE ATTACKER SHOWS A SET OF DUMMY BUTTONS OR LINKS, THEN LOADS ANOTHER PAGE OVER IT IN A TRANSPARENT LAYER. USERS THINK THEY ARE CLICKING ON THE VISIBLE PAGE WHILE THEY ARE ACTUALLY PERFORMING ACTIONS ON THE HIDDEN PAGE WHICH THE USERS NEVER INTENDED, SUCH AS CHANGING PRIVACY SETTINGS ON A SOCIAL NETWORKING SITE OR FOLLOWING SOMEONE ON TWITTER.
COMMERCIAL/THIRD PARTY SOCIAL MEDIA	SOCIAL MEDIA HOSTED ON SERVERS OVER WHICH DHS HAS NO CONTROL. THIS INCLUDES PROPRIETARY SOCIAL NETWORKING SITES SUCH AS FACEBOOK AND MYSPACE, AS WELL AS COLLABORATION SERVICES SUCH AS WIKIPEDIA, BLOGSPOT, AND DELICIOUS.
CONTENT MANAGER	ANY INDIVIDUAL DESIGNATED TO MANAGE WEB CONTENT FOR DHS OR A COMPONENT. THE DUTIES OF THE WEB CONTENT MANAGER INCLUDE ENSURING COMPLIANCE WITH ACCESSIBILITY STANDARDS FOR PERSONS WITH DISABILITIES. THIS INDIVIDUAL IS THE ORGANIZATION'S PRIMARY POINT OF CONTACT FOR WEB ISSUES.[8]
CONTENT PROVIDER	ANY INDIVIDUAL WHO CREATES CONTENT FOR PUBLICATION TO DHS WEBSITES.[9]
ENTERPRISE NETWORK	THE COMMUNICATIONS BACKBONE THAT INTERCONNECTS EVERY COMPUTER AND ASSOCIATED DEVICE AT EVERY LOCATION UNDER THE JURISDICTION OF AN ORGANIZATION, SUCH AS DHS.

[8] DHS 4300A, IV DEFINITIONS, J

[9] DHS 4300A, IV DEFINITIONS, K

EXTERNAL HOSTING	PROVISION BY AN EXTERNAL ORGANIZATION OR COMPANY OF ACCESS, ON A FEE-PER-SERVICE BASIS, TO THE EQUIPMENT, TECHNOLOGY AND SUPPORT TO NEEDED TO ESTABLISH AND RUN A WEBSITE, AS OPPOSED TO AN ORGANIZATION'S USING ITS OWN IN-HOUSE RESOURCES.
FARMING	SEE **PHARMING**
FISHING	SEE **PHISHING**
FOURSQUARE	A LOCATION-BASED SOCIAL NETWORKING WEBSITE AND APPLICATION FOR MOBILE DEVICES. USERS "CHECK IN" OR REPORT THEIR LOCATION BY ACCESSING A MOBILE WEBSITE, TEXT MESSAGING OR A DEVICE-SPECIFIC APPLICATION, SO THAT THEIR WHEREABOUTS CAN BE DISCOVERED BY OTHERS. FOURSQUARE ALSO INCORPORATES ELEMENTS OF A GAME BY AWARDING USERS POINTS FOR BEING THE FIRST TO VISIT A NEW PLACE, AND FOR ADDING NEW INFORMATION ABOUT THE LOCATIONS THEY VISIT.
HACKER	A PERSON WHO USES THEIR PROFICIENCY WITH ELECTRONICS, COMPUTERS AND/OR PROGRAMMING SKILLS TO GAIN ILLEGAL ACCESS TO OTHERS' DIGITAL RESOURCES, INCLUDING PERSONAL HANDHELD DEVICES, FILES, COMPUTERS AND NETWORKS.
INTERNET FOOTPRINT	THE COLLECTIVE ACTIVITIES AND BEHAVIORS RECORDED AS AN INDIVIDUAL INTERACTS IN A DIGITAL ENVIRONMENT, INCLUDING DEVICE USAGE, SYSTEM LOGINS AND LOGOUTS, WEBSITE VISITS, FILES, TRANSMITTED EMAILS, AND POSTED MESSAGES. "PASSIVE FOOTPRINTS" ARE CREATED WHEN DATA ARE COLLECTED ABOUT INDIVIDUALS' ACTIVITIES WITHOUT ANY DELIBERATE ACTION ON THEIR PART, SUCH AS TRACKING WHICH PRODUCTS CUSTOMERS ARE VISITING ON A VENDOR'S WEBSITE REGARDLESS OF WHETHER PURCHASES OCCUR. "ACTIVE FOOTPRINTS" ARE CREATED WHEN PERSONAL DATA IS RELEASED INTENTIONALLY BY INDIVIDUALS FOR THE PURPOSE OF SHARING INFORMATION WITH OTHERS ONLINE. FOOTPRINTS ARE SOMETIMES USED AS A ROUGH MEASURE OF AN INDIVIDUAL'S "WEB PRESENCE."
KEYSTROKE LOGGERS	ALSO CALLED A "KEYLOGGER," IT IS A HARDWARE DEVICE OR PROGRAM THAT MONITORS AND RECORDS EACH KEYSTROKE A USER TYPES ON A COMPUTING DEVICE'S KEYBOARD. ALTHOUGH SOMETIMES USED FOR LEGITIMATE PURPOSES, SUCH AS DIAGNOSTICS OR MONITORING A CHILD'S INTERNET ACTIVITY, A MORE TYPICAL USE OF KEYSTROKE LOGGERS IS FOR THE UNAUTHORIZED CAPTURE OF SECURITY CREDENTIALS SUCH AS PASSWORDS AND PERSONAL IDENTIFICATION NUMBERS.

MALWARE	DERIVED FROM THE PHRASE "MALICIOUS SOFTWARE," THIS TERM IS A GENERIC TERM FOR ANY PROGRAM WHOSE PURPOSE IS TO CAUSE HARM TO A COMPUTER SYSTEM. TYPICALLY, MALWARE IS INSTALLED WITHOUT THE USER'S KNOWLEDGE OR CONSENT, ALTHOUGH IT IS OFTEN PACKAGED WITH OTHER SOFTWARE THE USER DOES IN FACT CHOOSE TO INSTALL OR DOWNLOAD. VIRUSES AND WORMS ARE EXAMPLES OF MALWARE.
MASHUP	A WEB PAGE OR APPLICATION THAT ENABLES THE FAST, EASY COMBINATION OF DATA AND/OR FUNCTIONALITY FROM MULTIPLE SOURCES TO CREATE A NEW, ENRICHED RESULT THAT WAS NOT NECESSARILY THE REASON FOR PRODUCING THE ORIGINAL SOURCES. MOST MASHUPS USE PUBLICLY-ACCESSIBLE RESOURCES. FOR EXAMPLE, A MASHUP MIGHT SUPERIMPOSE ON A GOOGLE MAP OF A NEIGHBORHOOD THE AVERAGE HOUSING PRICES DRAWN FROM A CITY ASSESSOR'S ONLINE DATABASE.
METADATA	INFORMATION ABOUT THE MEANING OF OTHER INFORMATION. METADATA CAN DESCRIBE OR SUMMARIZE KEY ATTRIBUTES OF A PIECE OF INFORMATION TO FACILITATE FINDING THAT INFORMATION WHEN NEEDED. AN EXAMPLE OF METADATA IS A TIME STAMP THAT SPECIFIES WHEN A PIECE OF INFORMATION WAS CREATED.
MICRO-BLOG	EXTREMELY SHORT BLOG POSTS SIMILAR TO TEXT MESSAGING. THE MESSAGES CAN EITHER BE VIEWED BY ANYONE OR BY A RESTRICTED GROUP THAT IS CHOSEN BY THE USER. TWITTER, A POPULAR MICRO-BLOG CLIENT, ALLOWS POSTS OF UP TO 140 CHARACTERS TO BE UPLOADED AND READ USING INSTANT MESSAGING OR MOBILE DEVICES VIA TEXT MESSAGING.
PASSWORD ATTACK	AN ATTEMPT TO OBTAIN A LEGITIMATE USER'S PASSWORD. HACKERS CAN USE COMMON PASSWORD LISTS, DICTIONARIES, CRACKING PROGRAMS, AND PASSWORD SNIFFERS IN PASSWORD ATTACKS.
PERSONALLY IDENTIFIABLE INFORMATION (PII)	ANY INFORMATION THAT PERMITS THE IDENTITY OF AN INDIVIDUAL TO BE DIRECTLY OR INDIRECTLY INFERRED, INCLUDING OTHER INFORMATION THAT IS LINKED OR LINKABLE TO AN INDIVIDUAL.[10]
PHARMING	AN ACTION WHEREBY A HACKER SUBVERTS A USER'S ATTEMPT TO VISIT A LEGITIMATE WEBSITE BY INSTEAD REDIRECTING HIM OR HER TO A COUNTERFEIT OR "SPOOFED" WEBSITE. THE SPOOFED SITE IS DESIGNED TO TRICK USERS INTO REVEALING PERSONAL INFORMATION SUCH AS USERNAMES, PASSWORDS, AND ACCOUNT INFORMATION.

[10] DHS 4300A, IV DEFINITIONS, H

PHISHING	AN ATTEMPT TO FRAUDULENTLY ACQUIRE A USER'S PERSONAL INFORMATION, SUCH AS PASSWORDS AND CREDIT CARD DETAILS, BY MASQUERADING AS A TRUSTWORTHY PERSON OR BUSINESS IN AN APPARENTLY OFFICIAL ELECTRONIC COMMUNICATION. PHISHING IS COMMON IN E-MAIL AND INSTANT MESSAGING. FOR EXAMPLE, YOU MIGHT RECEIVE AN E-MAIL THAT APPEARS TO COME FROM AN OFFICIAL AT YOUR BANK THAT INSTRUCTS YOU TO "CONFIRM" YOUR INTERNET BANKING CREDENTIAL BY CLICKING ON A LINK. THE "SPOOFED" WEBSITE TO WHICH YOU WOULD BE DIRECTED WOULD CAPTURE YOUR CREDENTIALS IN ORDER TO ENABLE A THIRD PARTY TO ACCESS AND WITHDRAW ALL FUNDS FROM YOUR BANK ACCOUNT.
SOCIAL BOOKMARKING	A WEB-BASED SERVICE WHERE USERS CREATE AND STORE LINKS TO INFORMATION ON TOPICS OF PARTICULAR INTEREST TO THEM. ALTHOUGH WEB BROWSERS HAVE THE ABILITY TO BOOKMARK LINKS TO "FAVORITE" PAGES, THOSE LINKS ARE TIED TO AN INDIVIDUAL BROWSER ON A SINGLE COMPUTER. SOCIAL BOOKMARKING, BY CONTRAST, STORES LINKS IN AN ONLINE ACCOUNT WHICH CAN BE MADE PUBLIC. THESE BOOKMARKS CAN BE SHARED AND DISCOVERED BY OTHERS WHO ARE INTERESTED IN FINDING INFORMATION ON SIMILAR TOPICS. EXAMPLES OF SOCIAL BOOKMARKING SITES INCLUDE DELICIOUS, DIGG, AND REDDIT.
SOCIAL ENGINEERING	THE ACT OF DECEIVING OR TRICKING PEOPLE INTO PERFORMING ACTIONS OR DIVULGING CONFIDENTIAL INFORMATION, RATHER THAN OBTAINING SUCH INFORMATION BY BREAKING IN OR USING TECHNICAL MEANS. FOR EXAMPLE, SOMEONE POSING AS A HELP DESK REPRESENTATIVE MIGHT TELEPHONE YOU AND CLAIM TO BE DIAGNOSING A CONNECTION PROBLEM; THE CALLER REQUESTS THAT YOU VERIFY YOUR LOGIN ID AND PASSWORD OR OTHER PERSONAL INFORMATION SO IT CAN BE CHECKED AGAINST THE ITEMS ON FILE.
SOCIAL MEDIA	INTERNET-BASED APPLICATIONS THAT BUILD ON THE FOUNDATIONS OF WEB 2.0 TO ALLOW THE CREATION AND EXCHANGE OF USER-GENERATED CONTENT. SOCIAL MEDIA CAN TAKE MANY DIFFERENT FORMS, INCLUDING BUT NOT LIMITED TO WEB-BASED COMMUNITIES AND HOSTED SERVICES, SOCIAL NETWORKING SITES, VIDEO AND PHOTO SHARING SITES, WIKIS, BLOGS, PODCASTS, VIRTUAL WORLDS, SOCIAL BOOKMARKING, AND MANY EMERGENT TECHNOLOGIES.
SOCIAL NETWORKING SERVICES	WEB-BASED SERVICES THAT CONNECT PEOPLE WHO SHARE THE SAME INTERESTS AND/OR ACTIVITIES, OR WHO ARE INTERESTED IN EXPLORING THE INTERESTS AND ACTIVITIES OF OTHERS. SOCIAL NETWORKING SERVICES PROVIDE A VARIETY OF WAYS FOR USERS TO INTERACT. FOR EXAMPLE, FACEBOOK IS USED AS A PLACE TO SOCIALIZE WITH FRIENDS, WHEREAS LINKEDIN CATERS TO THOSE WHO WISH TO MAKE PROFESSIONAL CONNECTIONS.
SPAM	UNSOLICITED OR UNDESIRED ELECTRONIC MESSAGES. SPAM INCLUDES LEGITIMATE ADVERTISEMENTS, MISLEADING ADVERTISEMENTS, AND PHISHING MESSAGES—ANY UNSOLICITED MESSAGE CAN BE SPAM.

SPEAR FISHING	SEE **SPEAR PHISHING**
SPEAR PHISHING	A TECHNIQUE BY WHICH THE ATTACKER GENERATES AN E-MAIL MESSAGE OR PROMPTS LINKING TO A WEBSITE. THE ATTACK'S TARGET IS A SPECIFIC INDIVIDUAL OR SMALL GROUP. THE GOAL IS TO CONVINCE THE TARGETS TO TAKE ACTION, WHICH GIVES THE ATTACKER ACCESS TO THEIR SYSTEM BY PRESENTING THEM WITH TEXT, IMAGES, OR URLS THAT THEY COULD ACTUALLY EXPECT AND THEREFORE MISTAKE FOR LEGITIMATE.
SPOOFED WEBSITE	AN IMPOSTOR WEBSITE THAT MIMICS A REAL COMPANY'S WEBSITE IN ORDER TO STEAL PERSONAL INFORMATION FROM SITE VISITORS. VICTIMS ARE OFTEN DIRECTED TO THESE SPOOFED SITES THROUGH PHISHING E-MAILS. SPOOFED SITES CAN LOOK EXTREMELY CONVINCING, BUT OFTEN CONTAIN SMALL FLAWS SUCH AS SPELLING ERRORS OR "SLIGHTLY WRONG" LOGOS.
SPYWARE	ANY SOFTWARE THAT COVERTLY GATHERS USERS' INFORMATION THROUGH THEIR COMPUTING DEVICES AND/OR THEIR INTERNET CONNECTION WITHOUT THEIR KNOWLEDGE FOR UNAUTHORIZED USE. SPYWARE APPLICATIONS ARE TYPICALLY HIDDEN COMPONENTS THAT USERS INADVERTENTLY DOWNLOAD TOGETHER WITH LEGITIMATE MATERIAL. SPYWARE MAY GATHER INFORMATION SUCH AS E-MAIL ADDRESSES FOR ADVERTISING PURPOSES, OR EVEN PASSWORDS AND CREDIT CARD DATA.
TRUSTED INTERNET CONNECTIONS (TIC	A DHS INITIATIVE IMPLEMENTING OMB MEMORANDUM M-08-05, TO OPTIMIZE AND STANDARDIZE THE SECURITY OF INDIVIDUAL EXTERNAL NETWORK CONNECTIONS INCLUDING CONNECTIONS TO THE INTERNET, THAT ARE CURRENTLY IN USE BY THE FEDERAL GOVERNMENT. A "TIC" IS A PHYSICAL LOCATION AN AGENCY USES TO MEET THE OBJECTIVES OF THE TIC INITIATIVE.
TWITTER	A SOCIAL NETWORKING MICRO-BLOGGING SERVICE THAT ENABLES ITS USERS TO SEND AND READ OTHER USERS' MESSAGES, CALLED "TWEETS." USERS ("FOLLOWERS") MAY SUBSCRIBE TO ("FOLLOW") OTHER USERS' TWEETS. TWITTER IS SOMETIMES CALLED THE "SHORT MESSAGE SERVICE OF THE INTERNET" BECAUSE OF THE COMPATIBILITY OF ITS INTERFACE WITH SMART PHONES. TWEETS ARE LIMITED TO 140 CHARACTERS.
UNIFORM RESOURCE LOCATOR (URL	IN COMPUTING, THE IDENTIFIER THAT SPECIFIES WHERE A RESOURCE IS LOCATED AND THE MECHANISM FOR RETRIEVING IT. THE BEST-KNOWN EXAMPLE OF THE USE OF URLS IS FOR THE ADDRESSES OF WEB PAGES ON THE INTERNET, SUCH AS WWW.DHS.GOV.
VIDEO SHARING	WEBSITES ON WHICH USERS POST VIDEO THEY HAVE TAKEN FOR OTHERS TO VIEW AND COMMENT ON. SUCH SITES ALLOW VIEWERS TO "EMBED" OR DISPLAY OTHERS' VIDEO ON THEIR OWN SITES. YOUTUBE IS PROBABLY THE MOST WIDELY KNOWN VIDEO SHARING SITE.

VIRTUAL WORLD	ONLINE COMMUNITIES WHERE USERS OR THEIR DIGITAL REPRESENTATIONS (CALLED "AVATARS") CAN SOCIALIZE, CONNECT, AND INTERACT WITH ONE ANOTHER USING TEXT AND VOICE CHAT. THE TERM IS USED MORE SPECIFICALLY TO REFER TO AN ONLINE COMMUNITY SUCH AS SECOND LIFE THAT FEATURES A COMPUTER-BASED SIMULATED THREE-DIMENSIONAL ENVIRONMENT WHERE USERS CAN NOT ONLY INTERACT BUT ALSO CREATE AND USE VIRTUAL OBJECTS.
VIRUS	A FORM OF MALWARE THAT CAN COPY ITSELF AND SPREAD FROM ONE COMPUTER TO ANOTHER IN THE FORM OF EXECUTABLE CODE WHEN ITS HOST IS TAKEN TO A TARGET COMPUTER. FOR EXAMPLE, A USER MIGHT SEND AN INFECTED FILE OVER A NETWORK, OR CARRY IT ON A REMOVABLE MEDIUM SUCH AS A CD OR THUMB DRIVE, OR THE VIRUS MIGHT SEND AN INSTANT MESSAGE TO ALL THE CONTACTS ON THE INFECTED MACHINE WHICH, WHEN OPENED BY THE ADDRESSEE, INFECTS THE RECIPIENT'S COMPUTER. WHILE SOME VIRUSES ARE BENIGN, OFTEN A VIRUS WILL CAUSE A COMPUTER TO "HANG," RENDERING IT INOPERABLE BY CORRUPTING AND/OR DISABLING KEY OPERATING SYSTEM FILES AND TOOLS.
WEB 2.0	ALTHOUGH THERE IS NO AGREED-UPON DEFINITION OF THE TERM *WEB 2.0*, IT TERM GENERALLY REFERS TO THE MOVE TOWARD A MORE SOCIAL, INTERACTIVE, COLLABORATIVE, AND RESPONSIBLE WEB. IT CAN BE CHARACTERIZED BY CAPABILITIES AND TOOLS FACILITATING SOCIAL MEDIA DIALOG.
WHALING	PHISHING ATTACKS TARGETED AT HIGH-RANKING PERSONNEL IN AN ORGANIZATIONAL HIERARCHY, SUCH AS CHIEF EXECUTIVE OFFICERS (CEO) AND OTHER TOP EXECUTIVES.
WIDGET	A SELF-CONTAINED TOOL THAT CAN BE EMBEDDED IN A WEBSITE OR PROGRAM TO DELIVER A SINGLE-PURPOSE SERVICE, SUCH AS DISPLAYING THE LATEST NEWS AND WEATHER, MAPS, OR PHOTOS, OR ALLOWING A USER TO PLAY INTERACTIVE GAMES WITH OTHER WEBSITE VISITORS. USERS OF SOCIAL NETWORKING SITES OFTEN TAKE ADVANTAGE OF WIDGETS AS AN EASY WAY TO MAKE THEIR SITES MORE INTERESTING TO VISITORS; CARE MUST BE TAKEN, HOWEVER, SINCE HACKERS OFTEN USE WIDGETS AS MALWARE ENTRY POINTS.
WIKI	A TECHNOLOGY FOR CREATING COLLABORATIVE WEBSITES. FROM THE HAWAIIAN WORD MEANING "QUICK," A WIKI IS A COLLECTION OF WEB PAGES THAT ENCOURAGES USERS TO CONTRIBUTE OR MODIFY THE CONTENT. BY USING A SIMPLE WEB INTERFACE, A COMMUNITY CAN COLLABORATE TO DEVELOP A DOCUMENT OR WEB PAGE, NO MATTER WHERE THE MEMBERS OF THE COMMUNITY ARE LOCATED. BY FAR THE BEST-KNOWN WIKI IS WIKIPEDIA, A MULTILINGUAL, WEB-BASED, FREE CONTENT ENCYCLOPEDIA PROJECT.

WORM	SELF-REPLICATING MALWARE THAT USES A COMPUTER NETWORK TO SEND COPIES OF ITSELF FROM ONE COMPUTER SYSTEM TO ANOTHER. WORMS CAN CAUSE EXCESSIVE NETWORK TRAFFIC AND OTHER MALICIOUS DISRUPTIONS SUCH AS FILE DELETION AND SENDING JUNK MAIL TO EVERY E-MAIL ADDRESS IT DISCOVERS ON EVERY COMPUTER SYSTEM AS IT SPREADS THROUGHOUT A NETWORK.

REFERENCES

FEDERAL REGULATIONS

"STANDARDS OF ETHICAL CONDUCT FOR EMPLOYEES OF THE EXECUTIVE BRANCH," 5 CFR 2635

DHS MANAGEMENT DIRECTIVES (MD)

MD 0550.1, "RECORDS MANAGEMENT," MARCH 1, 2003

MD 4010.2, "SECTION 508 PROGRAM MANAGEMENT OFFICE AND ELECTRONIC AND INFORMATION TECHNOLOGY ACCESSIBILITY," OCTOBER 26, 2005

MD 4400.1, "DHS WEB (INTERNET, INTRANET, AND EXTRANET INFORMATION) AND INFORMATION SYSTEMS," MARCH 1, 2003

MD 4600.1," PERSONAL USE OF GOVERNMENT OFFICE EQUIPMENT," APRIL 14, 2003

MD 4900," INDIVIDUAL USE AND OPERATION OF DHS INFORMATION SYSTEMS/COMPUTERS," UNDATED

DHS PRIVACY OFFICE PUBLICATIONS

"DHS PRIVACY IMPACT ASSESSMENT FOR USE OF SOCIAL NETWORKING INTERACTIONS AND APPLICATIONS," DHS PRIVACY OFFICE, APRIL 2010

"GOVERNMENT 2.0: PRIVACY AND BEST PRACTICES: REPORT ON THE DHS PRIVACY OFFICE PUBLIC WORKSHOP, DHS PRIVACY OFFICE, NOVEMBER 2009

CONGRESSIONAL PROCEEDINGS

JOINT HEARING, "COLLECTION AND USE OF LOCATION INFORMATION FOR COMMERCIAL PURPOSES," U.S. HOUSE OF REPRESENTATIVES, ENERGY AND COMMERCE COMMITTEE, SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY AND THE INTERNET, AND SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION, FEBRUARY 24, 2010

OTHER GOVERNMENT SOURCES

"NEW MEDIA AND THE AIR FORCE," U.S. AIR FORCE PUBLIC AFFAIRS AGENCY, EMERGING TECHNOLOGY DIVISION, APRIL 6, 2009

"CIO COUNCIL GUIDELINES FOR SECURE USE OF SOCIAL MEDIA BY FEDERAL DEPARTMENTS AND AGENCIES," FEDERAL CIO COUNCIL, VERSION 1.0, SEPTEMBER 2009

GSA SOCIAL MEDIA POLICY AND HANDBOOK," CIO 2106.1, GENERAL SERVICES ADMINISTRATION, JULY 17, 2009

"SOCIAL MEDIA AND THE FEDERAL GOVERNMENT: PERCEIVED AND REAL BARRIERS AND POTENTIAL SOLUTIONS," FEDERAL WEB MANAGERS COUNCIL," DECEMBER 23, 2008

"SOCIAL MEDIA SECURITY MITIGATIONS," VERSION 1.1, U.S. CENTERS FOR DISEASE CONTROL AND PREVENTION, DECEMBER 3, 2009

ARTICLES AND WHITE PAPERS

"SECURITY THREAT REPORT: 2010," SOPHOS GROUP, 2010

"THE APPLICATION USAGE AND RISK REPORT: AN ANALYSIS OF END USER APPLICATION TRENDS IN THE ENTERPRISE," PALO ALTO NETWORKS, FALL 2009

"LOCATION-BASED SOCIAL MEDIA HAS LEGAL IMPLICATIONS FOR EMPLOYERS & EMPLOYEES," WWW.THESOCIALWORKPLACE.COM, APRIL 16, 2010

HTTP://WWW.NORWICH.EDU/ABOUT/NEWS/2007/011507-SOCIALNETWORK.HTML

[NOTE: THE FOLLOWING DOCUMENT IS PRESENTED IN ITS ENTIRETY AS ORIGINALLY ISSUED.]

DEPARTMENT OF HOMELAND SECURITY
MANAGEMENT DIRECTIVES SYSTEM MD
NUMBER: 4400.1
ISSUE DATE: 03/01/2003

DHS WEB (INTERNET INTRANET, AND EXTRANET INFORMATION) AND INFORMATION SYSTEMS

I. PURPOSE

THIS DIRECTIVE ESTABLISHES DEPARTMENT OF HOMELAND SECURITY (DHS) POLICY REGARDING DHS WEB (INTERNET, INTRANET, AND EXTRANET) AND INFORMATION SYSTEMS.

II. SCOPE

A. THIS DIRECTIVE APPLIES TO ALL DHS COMPONENTS.

B. THE SCOPE OF THIS DIRECTIVE IS LIMITED TO THE USE AND MANAGEMENT OF DHS WEB INFORMATION AND ASSOCIATED SYSTEMS WHERE THE INTENT IS TO MAKE INFORMATION AVAILABLE TO THE PUBLIC OR TO A GENERAL AUDIENCE WITHIN DHS. IT DOES NOT PERTAIN TO SPECIAL USE APPLICATIONS THAT HAPPEN TO USE THE WEB AS ALL OR PART OF THEIR COMMUNICATION NETWORK.

III. AUTHORITIES

THIS DIRECTIVE IS GOVERNED BY NUMEROUS PUBLIC LAWS AND AUTHORITIES, SUCH AS:

A. PUBLIC LAW 107-347, TITLE III, FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) OF 2002.

B. PUBLIC LAW 104-106. C. 5

U.S.C. 552A.

D. SECTION 508 OF THE REHABILITATION ACT OF 1973 AND IMPLEMENTING POLICY AND GUIDANCE.

E. THE FOLLOWING REGULATIONS AND DOCUMENTS REGARDING THE PRIVACY ACT:

1. ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986.

2. COMPUTER MATCHING AND PRIVACY PROTECTION ACT OF 1988.

3. PAPERWORK REDUCTION ACT OF 1995.

4. CHILDREN'S ONLINE PRIVACY PROTECTION ACT OF 1998.

5. OMB CIRCULAR NO. A-130, MANAGEMENT OF FEDERAL INFORMATION RESOURCES

6. OMB MEMORANDUM 99-05, INSTRUCTIONS ON COMPLYING WITH PRESIDENT'S MEMORANDUM OF MAY 14, 1998, "PRIVACY AND PERSONAL INFORMATION IN FEDERAL RECORDS".

7. OMB MEMORANDUM 99-18, PRIVACY POLICIES ON FEDERAL WEB SITES.

8. OMB MEMORANDUM 00-13, PRIVACY POLICIES AND DATA COLLECTION ON FEDERAL WEBSITES.

9. LETTER FROM JOHN SPOTILA TO ROGER BAKER, CLARIFICATION OF OMB COOKIES POLICY (SEPTEMBER 5, 2000).

IV. DEFINITIONS

FOR PURPOSES OF THIS DIRECTIVE, THE FOLLOWING DEFINITIONS APPLY.

A. ***CONTENT***: INFORMATION OF ANY KIND PUBLISHED TO THE WEB (INCLUDES TEXT, GRAPHICS, SYMBOLS, RETRIEVABLE DATA, AND PRESENTATION CONCEPTS).

B. ***DESIGNATED DHS OFFICIAL***: THE COMMANDANT OF DHS, THE INSPECTOR GENERAL, THE GENERAL COUNSEL, THE DIRECTOR OF THE SECRET SERVICE, THE DIRECTOR, BUREAU OF CITIZENSHIP AND IMMIGRATION SERVICES, THE PRIVACY OFFICER AND THE CIVIL RIGHTS OFFICER.

C. ***DHS ORGANIZATION HEADS***: SECRETARY, DEPUTY SECRETARY, ALL UNDERSECRETARIES, CHIEF OFFICERS AND DESIGNATED DHS OFFICIALS

D. ***EXTRANET***: ANY PRIVATE NETWORK THAT USES THE INTERNET PROTOCOL AND THE PUBLIC TELECOMMUNICATION NETWORKS TO SECURELY CONNECT TO DHS INTRANET AND ASSOCIATED SYSTEMS.

E. ***INTERNET***: THE PUBLICLY ACCESSIBLE WEB PRESENCE OF DHS. THE TOP-LEVEL (HOME) PAGE URL IS WWW.DHS.GOV.

F. ***INTRANET***: THE DHS WEB PRESENCE ONLY ACCESSIBLE VIA AUTHORIZED ACCESS TO DHS NETWORKS. NOTE THAT VARIOUS NON-DHS PERSONNEL MAY AT TIMES HAVE ACCESS TO THE DHS INTRANET.

G. ***PERSONAL USE***: ACTIVITY THAT IS CONDUCTED FOR PURPOSES OTHER THAN ACCOMPLISHING OFFICIAL OR OTHERWISE AUTHORIZED ACTIVITY.

H. **PERSONALLY IDENTIFIABLE INFORMATION**: ANY INFORMATION THAT PERMITS THE IDENTITY OF AN INDIVIDUAL TO BE DIRECTLY OR INDIRECTLY INFERRED, INCLUDING OTHER INFORMATION THAT IS LINKED OR LINKABLE TO AN INDIVIDUAL.

I. **PRIVACY ACT STATEMENT**: DISCLOSURE STATEMENT REQUIRED BY THE PRIVACY ACT TO APPEAR ON DOCUMENTS OR INTERFACES USED BY THE DEPARTMENT TO COLLECT PII FROM INDIVIDUALS TO BE MAINTAINED IN A PRIVACY ACT SYSTEM OF RECORDS.

H. ***SPECIAL USE APPLICATION***: DHS BUSINESS SOFTWARE THAT USES THE WEB AS ALL OR PART OF ITS COMMUNICATIONS NETWORK. GENERALLY HAS A LIMITED AUDIENCE AND RESTRICTED ACCESS VIA USER IDENTIFICATION/PASSWORD. THE FACT THAT A PARTICULAR APPLICATION MAY HAVE A VAST AUDIENCE (FOR EXAMPLE, A HUMAN RESOURCES APPLICATION ACCESSIBLE BY ALL EMPLOYEES) DOES NOT EXEMPT IT FROM THIS CATEGORY. SPECIAL USE APPLICATIONS ARE NOT SUBJECT TO THIS DIRECTIVE.

I. ***THE WEB***: REFERS TO THE INTERNET, INTRANET, AND EXTRANET COLLECTIVELY.

J. ***WEB CONTENT MANAGER***: ANY INDIVIDUAL DESIGNATED TO MANAGE WEB CONTENT FOR AN DHS OR A COMPONENT. THE DUTIES OF THE WEB CONTENT MANAGER INCLUDE ENSURING COMPLIANCE WITH ACCESSIBILITY STANDARDS FOR PERSONS WITH DISABILITIES. THIS INDIVIDUAL IS THE ORGANIZATION'S PRIMARY POINT OF CONTACT FOR WEB ISSUES.

K. ***WEB CONTENT PROVIDER***: ANY INDIVIDUAL WHO AUTHORS CONTENT FOR PUBLICATION TO DHS WEBSITES.

L. ***WEB PAGE***: ANY SINGLE DOCUMENT POSTED TO THE WEB.

M. ***WEB SITE***: A GROUP OR SYSTEM OF WEB PAGES GENERALLY RELATED BY THEIR CONTENT OR OWNERSHIP.

V. RESPONSIBILITIES

A. ***DHS WEB MANAGEMENT*** IS DIVIDED INTO THREE DISTINCT DISCIPLINES - MANAGEMENT OF WEB INFORMATION, MANAGEMENT OF ASSOCIATED SYSTEMS, AND MANAGEMENT OF SECURITY. ACCORDINGLY, THE RESPONSIBILITIES AND AUTHORITIES FOR EACH DISCIPLINE ARE ASSIGNED TO AN APPROPRIATE OFFICIAL. WITHIN THE DISCIPLINE OF INFORMATION MANAGEMENT, DIFFERENT OFFICIALS AND ENTITIES HAVE DISPARATE RESPONSIBILITIES.

B. ***THE WEB EXECUTIVE OVERSIGHT BOARD (WEOB)*** IS ESTABLISHED BY THIS DIRECTIVE AND SHALL BE COMPRISED OF MEMBERS FROM A BROAD CROSS-SECTION OF DHS ORGANIZATIONS, SUCH MEMBERS TO BE NOMINATED BY THE DHS ORGANIZATION HEAD. THE BOARD WILL:

1. PROVIDE DHS VISION AND DIRECTION FOR IMPLEMENTATION AND USE OF THE WEB.

2. BE CHAIRED BY THE DHS CHIEF INFORMATION OFFICER OR A SENIOR EXECUTIVE OFFICIAL DESIGNATED BY THE DHS CIO. THE WEOB CHAIR SHALL DESIGNATE AN INDIVIDUAL TO PERFORM ADMINISTRATIVE DUTIES RELATED TO WEOB ACTIVITIES.

3. BROKER AND REMEDIATE INTRADEPARTMENTAL CONCERNS AND CONFLICTS RELATED TO USE AND MANAGEMENT OF THE WEB.

4. HAVE THE AUTHORITY TO CHARTER WORKING GROUPS COMPRISED OF SELECTED MEMBERS OF DHS COMPONENTS AS NECESSARY.

C. ***THE UNDER SECRETARY FOR MANAGEMENT, THROUGH THE DHS CHIEF INFORMATION OFFICER***, SHALL BE RESPONSIBLE FOR ALL ASPECTS OF THIS DIRECTIVE.

D. ***THE DHS CHIEF INFORMATION OFFICER (CIO)*** SHALL:

1. PROVIDE OVERALL POLICY IMPLEMENTATION AND PROCEDURAL GUIDANCE FOR THE WEB AND ASSOCIATED SYSTEMS.

2. ENSURE ADHERENCE TO POLICIES, LAWS, REGULATIONS, AND GUIDANCE INCLUDING THOSE REGARDING ACCESSIBILITY, PRIVACY, AND SECURITY.

3. DEVELOP AND MAINTAIN THE INFORMATION SYSTEM SECURITY PLANS FOR WEB ASSOCIATED SYSTEMS. (WEB ASSOCIATED SYSTEMS REFER TO THOSE SYSTEMS THAT COMPRISE THE DHS WEB AND ARE NOT DIRECTLY ATTRIBUTABLE TO SPECIFIC PROGRAMS, SUCH AS WEB SERVERS, GATEWAYS, SECURITY SOFTWARE AND APPLIANCES AND OTHER ANCILLARY COMPONENTS.)

4. ESTABLISH AND ENFORCE TECHNICAL STANDARDS.

5. AUTHORIZE ALL DHS WEBSITES.

6. PROVIDE TECHNICAL PROCEDURAL GUIDANCE FOR ESTABLISHING AND MAINTAINING DHS WEBSITES.

7. SERVE AS EXECUTIVE SPONSOR OF THE WEB EXECUTIVE OVERSIGHT BOARD.

8. ESTABLISH A SINGLE INTERNET REPOSITORY FOR ALL DHS POLICY DEEMED RELEASABLE TO THE INTERNET.

E. ***THE DHS CHIEF INFORMATION SECURITY OFFICER (CISO)*** WITHIN THE DHS OFFICE OF THE CIO SHALL:

1. PROVIDE POLICY IMPLEMENTATION AND PROCEDURAL GUIDANCE REGARDING INFORMATION AND INFORMATION SYSTEM SECURITY FOR THE WEB.

2. ENSURE THAT DHS WEB INFORMATION AND ASSOCIATED SYSTEMS ADHERE TO LAWS, REGULATIONS, POLICIES, AND GUIDANCE REGARDING SECURITY.

3. REVIEW AND APPROVE THE INFORMATION SYSTEM SECURITY PLANS (ISSP) FOR WEB-ASSOCIATED SYSTEMS.

F. ***THE DHS ASSISTANT SECRETARY FOR PUBLIC AFFAIRS*** SHALL:

1. ENSURE THAT STYLE, MESSAGE, AND CONTENT ON THE INTERNET CONFORM TO THE DIRECTION AND VISION SET BY THE SECRETARY.

2. DESIGNATE A MEMBER TO THE WEB EXECUTIVE OVERSIGHT BOARD.

3. PROVIDE AND PUBLISH CONTENT DESCRIBING DHS'S MISSION, STATUTORY AUTHORITY, ORGANIZATIONAL STRUCTURE, AND STRATEGIC PLAN AS REQUIRED BY THE E-GOVERNMENT ACT OF 2002, AS AMENDED.

G. ***THE DHS HEADQUARTERS ORGANIZATION HEADS*** SHALL:

1. ENSURE PRIVACY COMPLIANCE ON ALL MATTERS RELATING TO WEB INFORMATION AND INFORMATION SYSTEMS.

2. ENSURE THAT WEBSITE INITIATIVES WITHIN THEIR RESPECTIVE AREAS OF RESPONSIBILITY ADHERE TO POLICIES, LAWS, REGULATIONS, AND GUIDANCE INCLUDING THOSE REGARDING ACCESSIBILITY, PRIVACY, AND SECURITY.

3. ESTABLISH A FORMAL PROCESS FOR PUBLISHING INFORMATION TO THE WEB THAT ACCOMMODATES THE REQUIREMENTS OF THIS DIRECTIVE AND APPLICABLE AUTHORITIES.

4. DEVELOP AND MAINTAIN CONTENT FOR THE WEB APPLICABLE TO THEIR SPECIFIC AREAS OF RESPONSIBILITY, AS THEY DEEM NECESSARY.

5. RESPOND TO CERTIFICATION AND REPORTING REQUIREMENTS FOR THEIR WEB INFORMATION AND ASSOCIATED SYSTEMS.

6. DESIGNATE A WEB CONTENT MANAGER.

7. DESIGNATE A MEMBER TO THE WEB EXECUTIVE OVERSIGHT BOARD. SUCH MEMBER WILL REPRESENT ALL AGENCY COMPONENTS WITHIN THE ORGANIZATION.

H. ***WEB CONTENT MANAGERS*** SHALL:

1. REVIEW AND APPROVE WEB CONTENT WITHIN THEIR AREA OF RESPONSIBILITY.

2. MANAGE WEB CONTENT INCIDENTS.

3. ENSURE THAT WEB CONTENT WITHIN THEIR AREA OF RESPONSIBILITY ADHERES TO LAWS, REGULATIONS, POLICIES, AND GUIDANCE INCLUDING THOSE REGARDING ACCESSIBILITY, PRIVACY, AND SECURITY.

I. ***WEB CONTENT PROVIDERS*** SHALL:

1. DEVELOP WEB CONTENT FOR PUBLICATION.

2. ADHERE TO LAWS, REGULATIONS, POLICIES, AND GUIDANCE, INCLUDING THOSE REGARDING ACCESSIBILITY, PRIVACY, AND SECURITY.

J. ***DHS EMPLOYEES*** SHALL:

1. COMPLY WITH THIS AND OTHER DIRECTIVES (INCLUDING MD 4600) PRESCRIBING USE AND MANAGEMENT OF WEB INFORMATION AND ASSOCIATED SYSTEMS.

2. REPORT DISCREPANCIES OR POLICY INCONSISTENCIES REFLECTED IN WEB CONTENT TO APPROPRIATE MANAGERS.

K. ***DHS EMPLOYEES*** SHALL NOT:

1. ACCESS PORNOGRAPHIC MATERIAL.

2. ACCESS STREAMING MEDIA FOR ENTERTAINMENT PURPOSES.

VI. POLICY & PROCEDURES

A. ***GENERAL***.

1. THE DEPARTMENT SHALL HAVE A SINGLE INTERNET HOME PAGE.

2. THE DEPARTMENT SHALL HAVE A SINGLE INTERNET REPOSITORY FOR ALL DHS POLICY DEEMED RELEASABLE TO THE INTERNET. DHS POLICY SHALL NOT BE REPEATED (DUPLICATED) ON OTHER DHS WEBSITES OR PAGES. LINKS TO THIS REPOSITORY OR TO SPECIFIC DOCUMENTS ARE PREFERRED AND APPROVED.

B. ***USE OF INTERNET RESOURCES***.

1. DHS WEBSITES AND PAGES SHALL BE ESTABLISHED ONLY FOR OFFICIAL, MISSION-RELATED OR MISSION SUPPORTING PURPOSES EXCEPT AS PROVIDED FOR BELOW.

2. LIMITED INCIDENTAL PERSONAL USE IS AUTHORIZED IN ACCORDANCE WITH MD 4600 AND WITH GOVERNMENT-WIDE POLICIES ON PERSONAL USE OF GOVERNMENT PROPERTY AND OFFICE EQUIPMENT.

3. DHS WEB SERVERS SHALL NOT BE USED TO HOST OR STORE WEB SITES OR PAGES NOT AUTHORIZED BY THE DHS CIO.

4. ALL ACTIVITIES SPONSORING WEB PAGES SHALL GIVE DUE CONSIDERATION AND MAKE EVERY EFFORT TO MINIMIZE THE USE OF BANDWIDTH BY THEIR WEB IMPLEMENTATIONS.

C. ***SECURITY/TERMS OF USE***.

1. THE DHS CISO IS THE AUTHORITY ON SECURITY MATTERS RELATING TO WEB INFORMATION AND ASSOCIATED SYSTEMS. THE CISO PROMULGATES MD 4300.1 WHICH ESTABLISHES DHS POLICY ON INFORMATION AND INFORMATION SYSTEM SECURITY. MD 4300.1 ESTABLISHES A FRAMEWORK FOR MANAGING THE SECURITY OF INFORMATION AND INFORMATION SYSTEMS. FOR THE PURPOSES OF THE ISS DIRECTIVE, THE WEB IS A GENERAL SUPPORT SYSTEM. INFORMATION REGARDING THE SECURITY LEVEL OF THE INTERNET, INTRANET, AND EXTRANET SYSTEMS AND CONTENT IS CURRENTLY BEING DEVELOPED AND WILL BE CONTAINED IN THE DHS WEB INFORMATION SYSTEM SECURITY PLAN.

2. A STANDARD SECURITY STATEMENT SHALL BE APPLIED DHS-WIDE AND SHALL BE READILY ACCESSIBLE FROM ALL TOP LEVEL, OR ENTRY POINT DHS WEB PAGES, OR AS DEEMED NECESSARY BY THE CISO.

3. ALL WEB INFORMATION AND INFORMATION SYSTEMS SHALL COMPLY WITH DHS MD # 4300 AND SUBSEQUENT AMENDMENTS.

D. ***PRIVACY***.

1. THE DHS CHIEF PRIVACY OFFICER IS THE AUTHORITY ON PRIVACY MATTERS RELATING TO WEB INFORMATION AND INFORMATION SYSTEMS. IN ADDITION TO THE POLICIES PRESCRIBED IN THE PRIVACY ACT OF 1974, SEVERAL OTHER GOVERNMENT-WIDE POLICIES AND GUIDANCE DOCUMENTS EXIST REGARDING PRIVACY RELATIVE TO THE WEB THAT SHOULD BE REFERENCED WHEN MAKING PRIVACY DETERMINATIONS. THEY ARE LISTED IN SECTION III OF THIS DIRECTIVE.

2. ALL WEB INFORMATION AND ASSOCIATED SYSTEMS SHALL COMPLY WITH PRIVACY ACT OF 1974 AND OTHER APPLICABLE LAWS, REGULATIONS, AND PRIVACY POLICIES.

3. A STANDARD PRIVACY STATEMENT SHALL BE APPLIED DEPARTMENT-WIDE AND SHALL BE READILY ACCESSIBLE FROM ALL TOP LEVEL, OR ENTRY POINT DHS WEB PAGES.

4. INFORMATION COLLECTION, USE, DISSEMINATION, AND MAINTENANCE SHALL BE IN COMPLIANCE WITH DHS'S STATED PRIVACY POLICY. THE CHIEF PRIVACY OFFICER MUST APPROVE EXCEPTIONS.

5. NO WEB PAGE SHALL BE USED TO GATHER INFORMATION FROM THE PUBLIC OR MONITOR PUBLIC USE OF THE DHS INTERNET WITHOUT THE EXPRESS AUTHORITY OF THE DHS PRIVACY OFFICER AND THE DHS CIO.

6. DHS PERSONNEL (EMPLOYEES, CONTRACTORS, ETC.) DO NOT HAVE A RIGHT, NOR SHOULD THEY HAVE AN EXPECTATION, OF PRIVACY WHILE USING THE WEB WHEN ACCESSED VIA GOVERNMENT COMPUTERS OR NETWORKS. ALL SUCH WEB ACTIVITIES ARE SUBJECT TO MONITORING AT ALL TIMES.

E. ***ACCESSIBILITY***.

1. THE DHS CIO IS THE AUTHORITY ON ACCESSIBILITY MATTERS RELATING TO WEB INFORMATION AND ASSOCIATED SYSTEMS FOR DHS.

2. ALL WEB INFORMATION AND ASSOCIATED SYSTEMS SHALL COMPLY WITH SECTION 508 OF THE REHABILITATION ACT OF 1973 AND ALL OTHER APPLICABLE DHS SPECIFIC AND GOVERNMENT-WIDE ACCESSIBILITY POLICIES.

3. THE POLICIES AND AUTHORITIES PRESCRIBED IN SECTION 508 OF THE REHABILITATION ACT OF 1973 AND IN MD 4010 SHOULD BE REFERENCED WHEN MAKING ACCESSIBILITY DETERMINATIONS.

F. ***CONTENT***.

1. A FUNDAMENTAL TENET OF THE E-GOVERNMENT ACT OF 2002 IS THAT GOVERNMENT AGENCIES MUST ESTABLISH A FORMAL PROCESS FOR DETERMINING WHAT INFORMATION TO PUBLISH TO THE WEB. HEADS OF DHS COMPONENTS ARE ASSIGNED THIS RESPONSIBILITY. THE PROCESS SHALL ALSO INCLUDE REVIEW AND APPROVAL MEASURES TO ENSURE COMPLIANCE WITH ALL LAWS, REGULATIONS, POLICIES, AND GUIDANCE INCLUDING THOSE REGARDING ACCESSIBILITY, PRIVACY, AND SECURITY.

2. ONLY OFFICIAL DESCRIPTIONS OF DHS MISSIONS AND ENTITIES SHALL BE USED ON DHS INTERNET WEBSITES.

3. DHS WEBSITES SHALL HAVE A MISSION ORIENTATION. A LINKAGE BETWEEN THE CONTENT AND DHS'S STRATEGIC GOALS AND OBJECTIVES SHOULD BE APPARENT.

4. INFORMATION SHALL ONLY BE PUBLISHED TO THE WEB BY PERSONS OR ENTITIES THAT CAN RIGHTFULLY BE CONSIDERED TO BE THE CONTROLLING AUTHORITY OF THE INFORMATION.

5. ALL DHS WEBSITES AND PAGES SHALL COMPLY WITH DHS AND GOVERNMENT-WIDE POLICY REGARDING RECORDS MANAGEMENT.

6. MANAGERS OF SITES OR PAGES THAT PROVIDE THE ABILITY TO CONTACT DHS WITH THE EXPECTATION OF A RESPONSE SHALL ENSURE THAT A MECHANISM IS IN PLACE TO PROVIDE AN ACCURATE RESPONSE WITHIN A REASONABLE TIMEFRAME - GENERALLY WITHIN THREE WORKING DAYS.

7. LINKS TO PAGES OUTSIDE OF DHS WEBSITES ARE AUTHORIZED IN SUPPORT OF VALID BUSINESS OBJECTIVES. LINKS MAY NOT ENDORSE A PARTICULAR NON-GOVERNMENTAL PRODUCT OR SERVICE OR PROVIDE PREFERENTIAL TREATMENT. NO PAYMENT OF ANY KIND SHALL BE ACCEPTED TO PROVIDE A LINK ON ANY DHS WEB PAGE TO ANOTHER WEB PAGE OR TO PROVIDE SPECIFIC CONTENT ON A DHS WEB PAGE.

8. THE FOLLOWING CATEGORIES OF INFORMATION ARE PROHIBITED ON DHS WEBSITES EXCEPT AS NOTED BY:

A. CLASSIFIED INFORMATION.

B. FOR OFFICIAL USE ONLY (FOUO) INFORMATION. C.

INFLAMMATORY COMMENTS.

D. INFORMATION PROTECTED UNDER THE PRIVACY ACT

E. ADVERTISEMENTS OR ENDORSEMENTS OF COMMERCIAL PRODUCTS OR SERVICES.

F. COPYRIGHTED OR TRADEMARKED MATERIAL WITHOUT EXPLICIT PERMISSION FROM THE AUTHOR OR NOT SUBJECT TO FAIR USE. "FAIR USE" IS A LEGAL CONCEPT THAT PERMITS THE USE OF COPYRIGHTED MATERIAL WITHIN CERTAIN LIMITATIONS, SUCH AS QUOTING A SHORT EXCERPT OF A PUBLICATION. ONLY LEGAL COUNSEL SHOULD MAKE FAIR USE DETERMINATIONS.

G. PERSONAL STATEMENTS REGARDING POLITICAL CANDIDATES, POLITICS OR OTHER POLITICAL STATEMENTS.

H. PORNOGRAPHIC MATERIAL.

I. INFORMATION REGARDING DHS PERSONNEL OR THEIR FAMILIES. NAMES AND DUTY ADDRESSES OF PERSONNEL ASSIGNED TO UNITS THAT ARE SENSITIVE, ROUTINELY DEPLOYABLE, OR STATIONED IN FOREIGN TERRITORIES WILL NOT BE RELEASED NOR WILL SUCH INDIVIDUALS BE IDENTIFIED IN PHOTOGRAPHS OR ARTICLES.[4]

J. INFORMATION THAT WOULD INTERFERE WITH AN OFFICIAL INVESTIGATION OR LAW ENFORCEMENT ACTIVITY, OR JUDICIAL PROCEEDING, INCLUDING INFORMATION THAT COULD SUBJECT LAW ENFORCEMENT PERSONNEL TO POTENTIAL HARM.

k. Internal program agenda, correspondence, and memos not appropriate for general distribution.

l. Pre-decisional information, reader files, internal letters, and memoranda shall not be released unless approved by the appropriate authority.

m. Procurement-sensitive or proprietary information.

n. Personal opinion or private agenda.

o. Duplication of DHS directives or other Government documents. p.

Links from DHS Internet sites to DHS Intranet sites.

q. Operations security (OPSEC) and Information Security (INFOSEC) material.

G. ***Exceptions to this Directive***: All exceptions to this Directive must be submitted by the DHS Component CIO in writing to the DHS CIO and will be handled on a case-by-case basis.

H. ***Questions or Concerns***: Any questions or concerns regarding this directive should be addressed to the Office of the DHS CIO.