Homeland Security

DHS 4300A

Sensitive Systems Handbook

Version 11.0

January 14, 2015

Protecting the Information that Secures the Homeland

This page intentionally left blank

FOREWORD

This Handbook and its Attachments provide guidance and best practices for implementation, and checklists of required and recommended measures that protect the security of DHS information.

The Handbook is based on the Department of Homeland Security (DHS) 4300 series of information security policies, which are the official documents that create and publish Departmental standards in accordance with DHS Management Directive 140-01 *Information Technology System Security*.

Comments concerning DHS Information Security publications are welcomed and should be submitted to the DHS Director for Information Systems Security Policy at infosecpolicy@hq.dhs.gov or addressed to:

DHS Director of Security Policy and Remediation
OCIO CISO Stop 0182
Department of Homeland Security
245 Murray Lane SW
Washington, DC 20528-0182

/S/

Jeffrey Eisensmith
Chief Information Security Officer
Department of Homeland Security

Contents

The following 4300A Sensitive Systems Handbook Attachments can be found at http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Pages/sspolicy.aspx#4300A

~~Attachment A—Requirements Traceability Matrix~~ [removed as of v9.1] [No longer published]

Attachment B—Waiver Request Form

Attachment C—Information Systems Security Officer Designation Letter

Attachment D—Type Authorization

Attachment E—FISMA Reporting

Attachment F—Incident Response and Reporting [UNDER REVISION]

Attachment G—Rules of Behavior

Attachment H—Plan of Action and Milestones (POA&M) Process Guide

~~**Attachment I—Workstation Logon, Logoff, and Locking Procedures**~~ **[removed as of v9.1] [No longer published]**

~~**Attachment J—Requesting Exceptions to Citizenship Requirement**~~ **[removed as of v10.1] [No longer published]**

Attachment K—IT Contingency Plan Template

~~**Attachment L—Password Management**~~ **[removed as of v10.1]. [No longer published]]**

Attachment M—Tailoring the NIST SP 800-53 Security Controls

Attachment N—Preparation of Interconnection Security Agreements

Attachment O—Vulnerability Assessment Program [UNDER REVISION]

Attachment P—Document Change Requests

Attachment Q1—Wireless Systems

Attachment Q2—Mobile Devices

Attachment Q3—Wireless Tactical Systems [UNDER REVISION]

Attachment Q4—Sensitive RFID Systems

Attachment Q5—Voice Over Internet Protocol (VoIP)

Attachment Q6—Bluetooth

Attachment R—Compliance Framework for CFO Designated Financial Systems

Attachment S—Compliance Framework for Privacy Systems

Attachment S1—Managing CREs Containing SPII

~~**Attachment T—Acronyms and Abbreviations**~~ **[removed as of v9.1] [No longer published; this Handbook and Attachments where required contain individual Acronym and Abbreviation lists.**

~~**Attachment U—Media Reuse**~~ **[removed as of v9.0] [No longer published]**

Attachment X—Social Media

Enclosure 1 content
(located at http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Pages/ITSecPolicy.aspx):

- DHS Cisco Router Configuration Guidance
- DHS SQL Server Configuration Guidance
- DHS Oracle Configuration Guidance

- DHS Active Directory Baseline Configuration
- DHS HP-UX Baseline
- DHS Solaris Baseline Configuration
- DHS Solaris 10 Baseline Configuration
- DHS Linux/SE Linux Configuration Guidance
- DHS Windows Vista Configuration Guidance
  - Appendix A: Vista Computer Configuration Security Settings
  - Appendix B: Vista Computer Configuration Other Settings
- DHS Windows XP Baseline Configuration
- DHS Windows Server 2003 Configuration Guidance
- DHS Windows Server 2008 Configuration Guidance
- DHS Windows 7 Configuration Guidance
- DHS Windows 8 Configuration Guidance
- NSA Guidance – Guide to Securing Microsoft Windows NT Network
  - Addendum – NSA Guide to Securing Microsoft Windows NT Networks & NSA Guides to Securing Windows 2000
- Guidance for Securing Windows NT and Server 2000
- Level One Benchmark Windows NT 4-0 Operating Systems V1.0.5
- Red Hat Linux Configuration

This page intentionally left blank

1.0 INTRODUCTION

This Handbook serves as the foundation on which DHS Components are to develop, build, and implement their information security programs; it provides specific techniques and procedures for implementing the requirements of the DHS Information Security Program for Sensitive Systems, and for meeting the Program's Baseline Security Requirements (BLSR), which are generated by the DHS information security policies published in DHS Sensitive Systems Policy Directive 4300A. Components must address these BLSRs when developing and maintaining information for their security documents.

A compilation is contained in this Handbook of best practices used by Department of Homeland Security (DHS) Components that adhere to DHS IT security policies and meet requirements contained in various National Institute of Standards and Technology (NIST) publications, Office of Management and Budget (OMB) direction, and Congressional and Executive mandates.

The scope and contents of this handbook will be updated as new capabilities are added to DHS systems, as security standards are upgraded, and as user experiences and needs change.

This handbook addresses only information security and is issued as implementation guidance under the authority of the DHS Chief Information Officer (CIO) through the Office of the DHS Chief Information Security Officer (CISO).

The aspects of information security covered by this Handbook are comprehensive; they pertain to personnel, physical, information, and industrial security; investigations; emergency preparedness; and domestic counterterrorism. Additional information will be published by the proponents of these programs.

1.1 Information Security Program and Implementation Guidelines

The DHS Information Security Program provides the baseline of policies, standards, and guidelines for DHS Components. This Handbook provides direction to managers and senior executives for managing and protecting sensitive systems. The sections in this Handbook are numbered parallel to the pertinent sections of DHS Sensitive Systems Policy Directive 4300A, where specific requirements and responsibilities are given.

This Handbook pertains to DHS Sensitive Systems as distinct from DHS National Security Systems (NSS). All DHS National Security Systems must use the guidance provided in the DHS National Security Systems Policy Directive 4300B series, dated, April 19, 2013, which are available on the DHS CISO website. The 4300B series applies to all DHS elements, employees, contractors, detailees, others working on behalf of DHS, and users of DHS NSS that collect, generate, process, store, display, transmit, or receive Confidential, Secret, or Top Secret classified national security information. The DHS National Security Systems Policy Directive 4300B series documents are available on the DHS CISO website.

Policy elements are effective when issued. Any policy element that has not been implemented within ninety (90) days is considered a weakness and either a system or program Plan of Action and Milestones (POA&M) must be generated by the Component for the identified weaknesses. When the Policy Directive is changed, the CISO will ensure that appropriate tool changes are made available to the Department within forty-five (45) days of the changes.

1.2 Authorities

The following list provides the authoritative references for the DHS sensitive information security program. Additional references are located in Appendix C of this document.

The following are authoritative references for the DHS sensitive information security program. Additional references are located in Appendix C to this Handbook.

- E-Government Act of 2002, including Title III, Federal Information Security Management Act (FISMA), 44 USC 3541Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Transmittal Memorandum 4, 2010
- DHS Management Directive MD 140-01, "Information Technology Systems Security," July 31, 2007
- National Institute of Standards and Technology (NIST) Federal Information Processing Standard FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006
- NIST Special Publication (SP) 800-53, Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013, with updates as of January 15, 2014

1.3 Handbook Overview

This Handbook provides guidance that for implementing the following controls required by DHS policy:

- **Management Controls** – These controls focus on managing both system information security controls and system risk. These controls consist of risk mitigation techniques normally used by management.
- **Operational Controls** – These controls focus on mechanisms primarily implemented and executed by people. Operational controls are designed to improve the security of a particular system or group of systems and often rely on management and technical controls.
- **Technical Controls** – These controls focus on security controls executed by information systems. Technical controls provide automated protection from unauthorized access or misuse; facilitate detection of security violations; and support security requirements for applications and data.
- **Privacy Controls** – DHS privacy controls have been added to DHS information security policy documents to comply with the publication of NIST SP 800-53, Rev.4, Appendix J: Privacy Control Catalogue. The privacy controls focus on information privacy as a value distinct from, but highly interrelated with, information security. Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of Personally Identifiable Information (PII).

1.4 Definitions

The definitions in this section apply to guidance provided in this document. Other definitions may be found in Handbook Overview?Committee on National Security Systems (CNSS) Instruction No. 4009, "National Information Assurance Glossary," 26 April 2010 and in *Privacy*

Incident Handling Guidance and privacy compliance documentation issued by the DHS Privacy Office.

1.4.1 Sensitive Information

Sensitive information is information not otherwise categorized that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security numbers; trade secrets; system vulnerability information; pre-solicitation procurement documents, such as statements of work; and information pertaining to law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies in internal controls are also sensitive information because of the potential damage that could be caused by the misuse of this information. System vulnerability information about a financial system is considered Sensitive Financial Information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access.

With the exception of certain types of information protected by statute (e.g. Sensitive Security Information, Critical Infrastructure Information), there are no specific Federal criteria and no standard terminology for designating types of sensitive information. Such designations are left to the discretion of each individual Federal agency. "For Official Use Only" (FOUO) is the term used within DHS to identify unclassified information of a sensitive nature that is not otherwise categorized by statute or regulation. DHS will adopt the term "Controlled Unclassified Information" (CUI) at a later date.

1.4.2 Public Information

This type of information can be disclosed to the public without restriction but requires protection against erroneous manipulation or alteration (e.g., public websites).

1.4.3 Classified National Security Information

Information that has been determined, pursuant to Executive Order 13526, "Classified National Security Information," to require protection against unauthorized disclosure and is marked to indicate its classified status.

1.4.4 National Intelligence Information

The following definition is provided in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law 108-458, 118 Stat. 3638:

> "The terms 'national intelligence' and 'intelligence related to national security' refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that – "(A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and "(B) that involves – (i) threats to the United States, its people, property, or interests; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on United States national or homeland security."

1.4.5 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 except for information on international terrorist activities.

1.4.6 Information Technology

Division E of the Information Technology Management Reform Act of 1996, Public Law 104-106, codified at 40 USC 1401 et seq., commonly referred to as the Clinger-Cohen Act of 1996, defines Information Technology (IT) as

> "any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an Executive agency."

For purposes of the preceding definition, "equipment" refers to that used by any DHS Component or contractor, if the contractor requires the use of such equipment in the performance of a service or the furnishing of a product in support of DHS.

The term *information technology* includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

The term *information system* as used in this policy document, is equivalent to the term *IT system*.

1.4.7 DHS System

A DHS system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local Government agency on behalf of DHS. DHS systems include *general support systems* and *major applications*.

1.4.7.1 General Support System

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 GSS 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.

Note: Security for GSSs in use at DHS Headquarters is under the oversight of the DHS Office of the Chief Information Officer (OCIO), with support from the DHS Security Operations Center (SOC). All other GSSs are under the direct oversight of respective Component CISOs, with support from the Component's SOC. Every GSS must have an Information Systems Security Officer (ISSO) assigned.

1.4.7.2 Major Application

A *major application* (MA) is an automated information system (AIS) that "requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or

unauthorized access to or modification of the information in the application.[1]" [Note: All Federal applications require some level of protection.] Certain applications, because of the information they contain, however, require special management oversight and should be treated as MAs. An MA is distinguishable from a GSS by the fact that it is a discrete application, whereas a GSS may support multiple applications. Each MA must be under the direct oversight of a Component CISO or Information System Security Manager (ISSM), and must have an ISSO assigned.

1.4.8 Component

A DHS *Component* is any organization which reports directly to the Office of the Secretary (including the Secretary, the Deputy Secretary, the Chief of Staff, the Counselors, and their respective staff, when approved as such by the secretary.

1.4.9 Trust Zone

A *Trust Zone* consists of 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). 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.

1.4.10 Continuity of Operations

Internal organizational efforts to ensure that a viable capability exists to continue essential functions across a wide range of potential emergencies, through plans and procedures that:

- Delineate essential functions and supporting information systems
- Specify succession to office and the emergency delegation of authority
- Provide for the safekeeping of vital records and databases
- Identify alternate operating facilities
- Provide for interoperable communications
- Validate the capability through tests, training, and exercises

1.4.11 Continuity of Operations Plan

A plan that provides for the continuity of essential functions of an organization in the event that an emergency prevents occupancy of its primary facility. It provides the organization with an operational framework for continuing its essential functions when normal operations are disrupted or otherwise cannot be conducted from its primary facility.

1.4.12 Essential Functions

Essential Functions are those that enable Executive Branch agencies to provide vital services, exercise civil authority, maintain the safety and well being of the general populace, and sustain industrial capability and the national economy base during an emergency.

[1] OMB Circular A-130

1.4.13 Vital Records

Vital records are Electronic and hardcopy documents, references, databases, and information systems needed to support essential functions under the full spectrum of emergencies. Categories of vital records may include:

- *Emergency operating records* – emergency plans and directive(s); orders of succession; delegations of authority; staffing assignments; selected program records needed to continue the most critical agency operations; and related policy or procedural records.
- *Legal and financial rights records* – records that protect the legal and financial rights of the Government and of the individuals directly affected by its activities. Examples include accounts receivable records, social security records, payroll records, retirement records, and insurance records. These records were formerly defined as "rights-and-interests" records.
- *Records used to perform national security preparedness functions and activities* in accordance with Executive Orders (EO).

1.4.14 Operational Data

Operational Data is any information used in the execution of any DHS mission.

1.4.15 Federal Information Security Management Act

The Federal Information Security Management Act (FISMA) requires each agency to develop, document, and implement an agency-wide information security program that will provide a high-level of security for the information and information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Statutory requirements include:

(1) Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.

(2) Policies and procedures that:

a. Are based on the risk assessments required by paragraph (1) above

b. Cost-effectively reduce information security risks to an acceptable level

c. Ensure that information security is addressed throughout the life cycle of each agency information system

d. Ensure compliance with

i. Other applicable Federal policies and procedures as may be prescribed by OMB and NIST Minimally acceptable system configuration requirements, as determined by the agency

ii. Any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President

(3) Subordinate plans for providing adequate information security for networks, facilities, and information systems, as appropriate;

(4) Security awareness training to inform personnel, including contractors, others working on behalf of DHS, and others who use information systems supporting operations and assets of the Department. Such training shall convey knowledge of

   a. Information security risks associated with their activities

   b. Their responsibility to comply with agency policies and procedures designed to reduce these risks

(5) Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually. This testing:

   a. Shall include testing of management, operational, and technical controls of every information system identified in the Department's inventory

   b. May include testing relied on by the Office of Inspector General (OIG)

(6) A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the Department's information security policies, procedures, and practices

(7) Procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines published by the United States Computer Emergency Readiness Team (US-CERT)

   a. Mitigating risks associated with incidents before substantial damage is done

   b. Notifying and consulting with US-CERT

   c. Notifying and consulting with:

      i. Law enforcement agencies and relevant OIG

      ii. An office designated by the President for any incident involving a national security system

      iii. Other agency or offices, as required

(8) Plans and procedures to ensure continuity of operations (CO) for information systems that support the operations and assets of the Department

FISMA requires that the CIO designate a senior agency information security official to develop and maintain a Department-wide information security program. The designee's responsibilities include:

- Developing and maintaining information security policies, procedures, and control techniques that address all applicable requirements
- Training and overseeing personnel with significant information security responsibilities
- Assisting senior Department officials with respect to their responsibilities under the statute
- Ensuring that the Department has sufficient trained personnel to ensure the Department's compliance with the statute and related policies, procedures, standards, and guidelines

- Ensuring that the Department CIO, in coordination with other senior Department officials, reports annually to the Secretary on the effectiveness of the Department's information security program, including the progress of remedial actions

1.4.16 Personally Identifiable Information

Personally Identifiable Information (PII) is any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, a visitor to the U.S., or a Department employee or contractor.

1.4.17 Sensitive Personally Identifiable Information

Sensitive PII is PII which if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of Sensitive PII include Social Security numbers, Alien Registration Numbers (A-Number), criminal history information, and medical information. Sensitive PII requires more stringent handling guidelines because of the greater sensitivity of the information.

1.4.18 Privacy Sensitive System

A *Privacy Sensitive System* is any system that collects, uses, disseminates, or maintains PII or Sensitive PII.

1.4.19 Strong Authentication

Strong authentication is a layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information.

1.4.20 Two-Factor Authentication

Authentication can involve something the user knows (e.g., a password), something the user has (e.g., a smart card), or something the user "is" (e.g., a fingerprint or voice pattern). *Single-factor authentication* uses only one of the three forms of authentication, while *two-factor authentication* uses any two of the three forms. *Three-factor authentication* uses all three forms.

1.5 Waivers

Components may request waivers to any portion of the requirements of DHS Sensitive Systems Policy Directive 4300A at any time they are unable to fully comply with a Policy Directive requirement. Waiver requests are routed through the Component's ISSO for the system to the Component's CISO or ISSM, and then to the DHS CISO. All submitters are to coordinate with the Authorizing Official (AO) prior to submission. If a material weakness is reported in an audit report, and the weakness is not scheduled for remediation within twelve (12) months, the Component must submit a waiver request to the DHS CISO. If the material weakness is in a financial system, the Component Chief Financial Officer (CFO) must also approve the waiver request before sending to the DHS CISO. If the material weakness is a privacy control, the DHS Chief Privacy Officer must also approve the waiver request before sending to the DHS CISO.

In all cases, waivers are to be requested for an appropriate period based on a reasonable remediation strategy.

1.5.1 Waiver Requests

The Waiver Request Form found in Attachment B of the *DHS 4300A Sensitive Systems Handbook* is used to request waivers from 4300A Policy requirements.

Component ISSOs, audit liaisons, and others may develop the waiver request, but the System Owner submits the request through the Component's CISO/ISSM.

Waiver requests are to include documentation of mission impact as operational justification; mission impact, risk acceptance; risk mitigation measures; and a POA&M for bringing the system procedures or control weakness into compliance.

Any waiver requests for CFO Designated Systems must be submitted to and approved by the Component's CFO prior to submission to the DHS CISO. Any waiver request for Privacy Sensitive Systems must be submitted to and approved by the Component's Privacy Officer or senior Privacy Point of Contact (PPOC) prior to being submitted to the DHS CISO.

Any waiver for compliance with privacy controls must be submitted to and approved by the DHS Chief Privacy Officer.

All approved waiver requests must be directed through the Component's CISO/ISSM who will in turn direct them to the DHS CISO.

1.5.2 Requests for Exception to U.S. Citizenship Requirement

Special procedures apply for exception to the requirement that persons accessing DHS systems be U.S. citizens. Under normal circumstances, only U.S. citizens are allowed access to DHS systems and networks; but there is a need at times to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to citizenship requirements are treated differently from security policy waivers. Exceptions to the U.S. citizenship requirement should be requested by completing a Foreign National Visitor Access Request, DHS Form 11052-1, which is available online or through the DHS Office of the Chief Security Officer (OCSO). Components who have access to the DHS OCSO Integrated Security Management System's (ISMS), Foreign National Vetting Management System (FNVMS) may file their requests in that manner. For further information regarding the citizenship exception process, contact the DHS OCSO at *foreign.visitors@hq.dhs.gov*.

1.6 Electronic Signature

Pursuant to Sections 1703 and 1705 of the Government Paperwork Elimination Act (GPEA), OMB Memorandum M-00-10, "Procedures and Guidance on Implementing of the Government Paperwork Elimination Act,"[2] requires executive agencies to provide the option for electronic maintenance, submission, and disclosure of information when practicable as a substitute for paper, and to use and accept electronic signatures.

Electronic signatures are essential in the Department's business processes and IT environments; reducing reliance on paper transactions improves information sharing, strengthens information security, and streamlines business processes, while reducing both cost and environmental impact.

[2] *Government Paperwork Elimination Act (GPEA), Pub L 105-277, 44 USC 3501 (note)provide for the use*

Electronic signature solutions must be approved by the Component CISO.

1.7 Information Sharing

The DHS SOC exchanges information with Component SOCs, Network Operations Centers (NOC), 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, accounting, performance, and security data. This data is monitored, collected, analyzed, processed, and reported by the NOCs and SOCs.

The DHS SOC is responsible for communicating other information such as incident reports, notifications, vulnerability alerts and operational statuses to Component SOCs, Component CISOs/ISSMs and other identified Component points of contact.

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

- Entering incident information into the DHS SOC 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

1.8 Threats

Emphasis on e-Government has added the general public to the class of Government computer users and has transferred the repository for official records from paper to electronic media.

Information systems are often connected to different parts of an organization; interconnected with other organizations' systems; and with the Internet. Remote access for telecommuting and building management services including but not limited to badge systems; heating, ventilating, and air-conditioning (HVAC); and entry may require additional connections, all of which introduce additional risks.

Wireless mobile systems such as cell phones and pagers allow personnel to stay in touch with their offices and wireless local area networks (WLAN) permit connection from various locations throughout a building. While these technologies provide greater flexibility and convenience, they also introduce additional risks.

As technologies continue to converge, (cell phones with Internet access, walkie-talkie communications, and video; low cost Voice over Internet Protocol [VoIP]; copiers that allow network printing; printing over the Internet; and facsimile [fax] functions) operating costs are reduced, making their implementation tempting; but each of these technology advancements contains inherent security risks and presents challenges to security professionals.

1.8.1 Insider Threats

Managers are generally aware of natural and physical threats, such as earthquakes, tornadoes, fires, floods, electric outages, and plumbing disasters, but may not have the same level of awareness regarding disasters or threats originating from within their organizations. The threat from DHS users should not be underestimated. Sensitive data can be lost, corrupted, or compromised through malicious or careless acts. A malicious user can intentionally cause harm to the Department's reputation and data. Uninformed or careless users can inflict similar damage.

Converging technologies combine the vulnerabilities of the individual technologies, so care must be taken to ensure that systems are designed with no single points of failure. (For example, if the building HVAC were connected to the data network it would become necessary to ensure that an outage or attack on the HVAC would not also cause a network outage.)

1.8.2 Criminal Threats

Malicious code remains a threat to DHS systems. Malware and those who employ it have become very sophisticated; malicious code can be tailored to the recipient. This code can be transferred to an unsuspecting user's machine by various means, including email, visiting infected websites, or across a network. These capabilities may be used to steal, alter, or destroy data; export malicious code to other systems; add backdoors that would permit access to data or network resources; or prevent the legitimate use of the individual computer or network service.

Instructions for exploiting hardware or software vulnerabilities are often available on hacker sites within hours of discovery. Skilled hackers routinely target e-commerce sites to obtain credit card numbers. Persons with hacking skills are often hired to perform espionage activities.

1.8.3 Foreign Threats

Foreign Governments routinely conduct espionage activities to obtain information that will be useful to their own industrial/government base and operations. They also have the resources to disrupt Internet communications and have launched successful cyber-attacks.

Eavesdropping on wireless communications with commercially available equipment is common; it is relatively easy to detect and exploit wireless access points. Employees overseas should assume that their wireless communications (BlackBerry, cell phone, etc.) are being monitored.

Many software manufacturers outsource software code development, which raises concerns about whether malicious or criminal code has been inserted. Indeed, it is becoming increasingly difficult to determine the actual provenance of an organization's information systems because code and equipment are assembled from so many sources.

1.8.4 Lost or Stolen Equipment

Lost or stolen equipment also poses a threat. Data on portable computing devices (laptops, smart phones, etc.) or storage media (Universal Serial Bus (USB) drives, compact disks (CD), etc.) can reveal sensitive information, such as changes to legislation, investigations, or economic analyses. Thefts from offices, airports, automobiles, and hotel rooms occur regularly.

1.8.5 Supply Chain Threats

A *supply chain threat* is a man-made threat achieved through exploitation of the system's supply chain or acquisition process.

A system's *supply chain* is composed of the organizations, people, activities, information, resources, and facilities for designing, creating and moving a product or service from suppliers through to the integrated system (including its sub-components), and into service by the original acquirer.

1.9 Changes to this Handbook, and Requests for Changes

The Handbook serves as a foundation for Components to use in developing and implementing their information security programs.

For interpretation or clarification of DHS information security guidance found in this Handbook or in DHS Sensitive Systems Policy Directive 4300A, contact the DHS CISO at infosecpolicy@hq.dhs.gov.

Changes to this policy and to the Handbook may be requested by submitting to the respective ISSM/CISO the form included in *DHS 4300A Sensitive Systems Handbook,* Attachment P, "Document Change Requests."

.

2.0 ROLES AND RESPONSIBILITIES

Security is inherently a Government responsibility; contractors, others working on behalf of the Department of Homeland Security (DHS), and other sources may assist in the performance of security functions, but a DHS employee must always be designated as the responsible agent for all security requirements and functions. This section outlines the roles and responsibilities for implementing these requirements.

2.1 Information Security Program Roles

Designated personnel play a major role in the planning and implementation of information security requirements. Roles directly responsible for information system security are described in the subsections that follow.

2.1.1 DHS Senior Agency Information Security Officer

The DHS CISO acts as the DHS Senior Agency Information Security Officer.

2.1.2 DHS Chief Information Security Officer

The DHS CISO implements and manages the DHS Information Security Program to ensure compliance with applicable Federal laws, Executive Orders, directives, policies, and regulations.

The DHS CISO reports directly to the DHS Chief Information Officer (CIO) and is the principal advisor on information security matters.

- The DHS CISO Implements and manages the Department-wide Information Security Program and ensures compliance with the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) directives, and other Federal requirements.
- Issues Department-wide information security policy, guidance, and architecture requirements for all DHS systems and networks. These policies incorporate National Institute of Standards and Technology (NIST) guidance, as well as all applicable OMB memorandums and circulars.
- Facilitates development of subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems.
- Serves as the principal Departmental liaison with organizations outside DHS in matters relating to information security.
- Establishes and institutionalizes contact with selected groups and associations within the security community:
  a. To facilitate ongoing security education and training for organizational personnel;
  b. To maintain currency with recommended security practices, techniques, and technologies; and
  c. To share current security-related information including threats, vulnerabilities, and incidents.
- Implements an insider threat program that includes a cross-discipline insider threat incident handling team.

- Establishes an information security workforce development and improvement program.
- Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems: 1. Are developed and maintained; and 2. Continue to be executed in a timely manner.
- Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
- Implements a threat awareness program that includes a cross-organization information-sharing capability.
- Reviews and approves the tools, techniques, and methodologies planned for use in certifying and authorizing DHS systems, and for reporting and managing systems-level FISMA data. This responsibility includes reviews and approval of Security Control Assessment plans, Contingency Plans, and security risk assessments.
- Consults with the DHS Chief Security Officer (CSO) on matters pertaining to physical security, personnel security, information security, investigations, and Sensitive Compartmented Information (SCI) systems, as they relate to information security and infrastructure.
- Develops and implements procedures for detecting, reporting, and responding to information security incidents.
- Ensures preparation and maintenance of plans and procedures to provide continuity of operations (CO) for information systems.
- Ensures that Department personnel, contractors, and others working on behalf of DHS receive information security awareness training.
- Chairs the CISO Council. The Council is composed of all Component CISOs, and is the Department's sole coordination body for any issues associated with information security policy, management, and operations. Component Information Systems Security Managers (ISSM) will be invited to CISO Council meetings as required.
- Maintains a comprehensive inventory of all general support systems (GSS) and major applications (MA) in use within the Department.
    - Security management for every GSS is under the direct oversight of either the DHS CISO (for enterprise systems) or a Component CISO/ISSM (for Component-specific GSSs).
    - MAs must be under the direct control of either a Component CISO or Component ISSM.
- Maintains a repository for all Information Assurance (IA) security authorization process documentation and modifications.
- Performs security reviews for all planned information systems acquisitions over $2.5 million and for additional selected cases.
- Provides oversight of all security operations functions within the Department.
- Maintains classified threat assessment capability in support of security operations.
- Performs annual program assessments for each of the Components.

- Performs periodic compliance reviews for selected systems and applications.
- Publishes monthly Compliance Scorecards.
- Delegates specific authorities and assigns responsibilities to Component CISOs and ISSMs, as appropriate for maintaining a high degree of compliance Reports annually to the Secretary on the effectiveness of the Department information security program, including progress of remedial actions. The CISO's annual report provides the primary basis for the Secretary's annual report to both OMB and to the United States Congress that is required by FISMA.
- Assists senior Department officials concerning their responsibilities under FISMA.
- Heads an office with the mission and resources to assist in ensuring Department compliance with information security requirements.
- Appoints a DHS employee to serve as the Headquarters CISO.
- Appoints a DHS employee to serve as the Office of Intelligence and Analysis (I&A) CISO.
- Provides operational direction to the DHS Security Operations Center (SOC).

2.1.3 Component Chief Information Security Officer

The Component CISO implements and manages all aspects of the Component Information Security Program to ensure compliance with DHS policy and guidance implementing FISMA, other laws, and Executive Orders. The Component CISO reports directly to the Component CIO on matters relating to the security of Component information systems. In order to ensure continuity of operations and effective devolution, large Components should ensure the designation of a Deputy CISO with full authorities, to include the roles of Risk Executive and Security Control Assessor upon the absence of the CISO.

The following Components are to have a fulltime CISO:

- Customs and Border Protection (CBP)
- Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- United States Secret Service (USSS)
- United States Coast Guard (USCG)
- Federal Emergency Management Agency (FEMA)
- United States Citizenship and Immigration Services (USCIS)
- Federal Law Enforcement Training Center (FLETC)
- Headquarters, Department of Homeland Security
- Office of Intelligence and Analysis (I&A)
- National Protection and Programs Directorate (NPPD)
- Science and Technology (S&T)

Component CISOs:

- Serve as principal advisor on information security matters
- Report directly to the Component CIO on matters relating to the security of Component information systems
- Oversee the Component information security program
- Ensure that information security-related decisions and information, including updates to the 4300 series of information security publications, are distributed to the ISSOs and other appropriate persons within their Component
- Approve and/or validate all Component information system security reporting
- Consult with the Component Privacy Officer or Privacy Point of Contact (PPOC) for reporting and handling of privacy incidents
- Manage information security resources including oversight and review of security requirements in funding documents
- Review and approve the security of hardware and software prior to implementation into the Component SOC
- Provide operational direction to the Component SOC
- Periodically test the security of implemented systems
- Implement and manage a Plan of Action and Milestones (POA&M) process for remediation by creating a POA&M for each known vulnerability
- Ensure that ISSOs are appointed for each information system managed at the Component level, and review and approve ISSO appointments
- Ensure that weekly incident reports are submitted to the DHS Security Operations Center (SOC)
- Acknowledge receipt of Information System Vulnerability Management (ISVM) messages, report compliance with requirements or notify the granting of waivers
- Manage Component firewall rule sets
- Ensure that Interconnection Security Agreements (ISA) are maintained for all connections between systems that do not have the same security policy
- Ensure execution of the DHS Logging Strategy detailed in this Handbook
- Ensure adherence to the DHS Secure Baseline Configuration Guides (Enclosure 1 to this Handbook)
- Ensure reporting of vulnerability scanning activities to the DHS SOC, in accordance with *DHS 4300A Sensitive Systems Handbook* Attachment O, "Vulnerability Management Program."
- Develop and maintain a Component-wide information security program in accordance with Department policies and guidance

- Implement Department information security policies, procedures, and control techniques to ensure that all applicable requirements are met
- Update Security Training section within DHS FISMA Manager resource at least once per quarter
- Ensure training and oversight of personnel with significant responsibilities for information security
- Oversee the Component's Security Authorization process for GSSs and MAs
- Maintain an independent Component-wide assessment program to ensure that there is a consistent approach to controls effectiveness testing
- Ensure that an appropriate SOC performs an independent network assessment as part of the assessment process for each authorized application
- Ensure that enterprise security tools are utilized
- Oversee all Component security operations functions, including the Component SOCs
- Ensure that external providers who operate information systems on behalf of the Component meet the same security requirements as required for information and information systems.
- Ensure an acceptable level of trust in the external service; or using compensating controls to secure information or the process flow, accepting a greater degree of risk, or reducing the functionality to the extent necessary to make the risk acceptable

Component CISO qualifications include:

- Training, experience, and professional skills required to discharge the responsibilities and functions of the position
- Ability to maintain a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance
- Ability to perform information security duties as primary duty
- Ability to participate in the DHS CISO Council
- Ability to head an office with the mission and resources to ensure the Component's compliance with this Policy Directive
- Ability to coordinate, develop, implement, and maintain an organization-wide information security program
- Ability to serve as the Component Risk Executive

2.1.4 Component Information Systems Security Manager

Components that are not required to have a fulltime CISO must have a fulltime ISSM. The ISSM is designated in writing by the Component CIO, with the concurrence of the DHS CISO.

The ISSM plays a critical role in ensuring that the DHS Information Security Program is implemented and maintained throughout the Component.

Component ISSMs:

- Oversee the Component information security program

- Ensure that the Component CIO and DHS CISO are kept informed of all matters pertaining to the security of information systems
- Ensure that all communications and publications pertaining to information security, including updates to the 4300 Policies and Handbooks, are distributed to the ISSOs and other appropriate persons within their Component
- Validate all Component information system security reporting
- Consult with the Component Privacy Officer or PPOC for reporting and handling of privacy incidents
- Manage information security resources including oversight and review of security requirements in funding documents
- Test the security of the Component's information systems periodically
- Implement and manage a POA&M process for remediation by creating a POA&M for each known vulnerability
- Ensure that ISSOs are appointed for each Component-managed information system
- Ensure that weekly incident reports are forwarded to the HQ CISO
- Acknowledge receipt of ISVM messages, report compliance with requirements, or notify applicants of the granting of waivers
- Ensure adherence to the DHS Secure Baseline Configuration Guides (Enclosure 1, *DHS 4300A Sensitive Systems Handbook*)
- Develop and publish procedures for implementation of DHS information security policy within the Component
- Implement Department information security policies, procedures, and control techniques to address all applicable requirements
- Ensure training and oversight for personnel with significant responsibilities for information security
    - Oversee the Security Authorization process for the Component's MAs.
    - Maintain an independent Component-wide security control assessment program to ensure a consistent approach to controls effectiveness testing
    - Ensure that an appropriate SOC performs an independent network assessment as part of the security control assessment process for each authorized application
    - Ensure that enterprise security tools are used

2.1.5 Risk Executive

A Risk Executive ensures that risks are managed consistently across the organization. In keeping with its organizational structure, DHS has two levels of Risk Executive: Departmental and Component. The risk executive provides a holistic view of risk beyond that associated with the operation and use of individual information systems. Risk Executive observations and analyses are documented and become part of the security authorization decision.

All DHS Risk Executives:

- Ensure that management of security risks related to information systems is consistent throughout the organization; reflects organizational risk tolerance; and is performed as part of an organization-wide process that considers other organizational risks affecting mission and business success
- Ensure that information security considerations for individual information systems, including the specific authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization
- Provide visibility into the decisions of AOs and a holistic view of risk to the organization beyond the risk associated with the operation and use of individual information systems
- Facilitate the sharing of security-related and risk-related information among AOs and other senior leaders in the organization in order to help those officials consider all types of risks that could affect mission and business success and the overall interests of the organization at large

The DHS Risk Executive develops information security policy, establishes the standards for system security risk, oversees risk management and monitoring, and approves all waivers to DHS policy.

Component Risk Executives may establish system security risk standards more stringent than DHS standards. Risk Executives implement the system security risk management and monitoring program and submit requests for higher-risk deviations from the enterprise standard.

2.1.6 Authorizing Official

The AO formally assumes responsibility for operating an information system at an acceptable level of risk. He or she is to be a senior management official and a Federal employee or member of the U.S. military. The AO assigns the Security Control Assessor for the system.

2.1.7 Security Control Assessor

The Security Control Assessor is a senior management official whose responsibilities include certifying the results of the security control assessment. A Security Control Assessor, who must be a Federal employee, is assigned in writing to each information system by an appropriate Component official, typically the Component Head or Component CIO. The Security Control Assessor and the team conducting a certification must be impartial. They must be free from any perceived or actual conflicts of interest with respect to the developmental, operational, and or management chains of command associated with the information system; or with respect to the determination of security control effectiveness.

For systems with low impact, a Security Control Assessor and/or certifying team does not need to be independent so long as assessment results are carefully reviewed and analyzed by an independent team of experts to validate their completeness, consistency, and truthfulness.

The AO decides the required level of assessor independence based on:

- The criticality and sensitivity of the information system
- The ultimate risk to organizational operations, organizational assets, and individuals

- The level of assessor independence required for confidence that the assessment results are sound and valid for making credible risk-based decisions.

2.1.8 Information Systems Security Officer

An ISSO performs security actions for an information system. There is only one ISSO designated to a system, but multiple Alternate ISSOs may be designated to assist the ISSO.

While the ISSO performs security functions, the System Owner is always responsible for information system security.

See Attachment C to this Handbook, "Information Systems Security Officer (ISSO) Designation Letter."

2.1.9 Ongoing Authorization Manager and Operational Risk Management Board

Each Component has an OA Manager responsible for evaluating and tracking security events for systems operating under the DHS OA Program. Component OA Managers:

- Account for Component risk threshold
- Ensure that Component Risk Executives [2.15] are made aware of new risks and security issues
- Facilitate collaboration of the Component IT Security SMEs that serve on the Operational Risk Management Board (ORMB)

Component ORMBs determine the criticality of security triggers and the impact of triggers on the security posture of Component systems that are in OA. The ORMB determines the level of each trigger's visibility and recommends to the Component CISO and AO as adjudicators the actions required to mitigate the risks introduced.

2.1.10 DHS Security Operations Center

The DHS Enterprise SOC (DHS SOC) is charged to act as a single point for DHS enterprise-wide cyber situational awareness. As such, DHS Enterprise SOC provides incident management oversight for all incidents detected and reported from all sources. DHS Enterprise SOC also provides the first line of active defense against all cyber threats by monitoring all perimeter network gateways. Lastly, DHS Enterprise SOC oversees the department-wide vulnerability management program.

The DHS SOC has functional, advisory, and reporting responsibilities that include the following:

- Review all reported incidents and verify that all pertinent information is recorded, confirmed, and that closure occurs only after all remediation and reporting activities have occurred in accordance with this SSPD 4300A.
- Focus 24x7 monitoring efforts on shared DHS infrastructure such as the Trusted Internet Connections (TIC), Policy Enforcement Points (PEP), E-mail Security Gateway (EMSG), Demilitarized Zones (DMZ), Virtual Private Networks (VPN) and other devices as required by DHS CISOs to identify security events of interest that require confirmation, escalation, or declaration as false positive.
- Create SENs based on monitoring and analysis activities when events of interest are identified that require further investigation.

- Provide oversight on investigational activities and review SENs prior to escalation. SENs will be escalated when Components have sufficiently demonstrated that adequate investigation has been performed and that the event is a verified incident. The Component must provide necessary information regarding the event in accordance with the escalation criteria outlined in Appendix F3, "Response Guidelines".
- Review all SENs for closure and close SENs after all reasonable investigational activities have been completed.
- Conduct operations and maintenance and approve changes on all security monitoring devices associated with shared DHS infrastructure (such as Intrusion Detection System (IDS), Data Loss Prevention (DLP).
- Provide oversight and guidance for all incidents to ensure adherence to DHS Sensitive Systems Policy Directive 4300A.
- Serve as the primary clearinghouse and collection point for information related to incidents involving DHS systems or networks.
- Coordinate privacy and security incident handling activities with DHS entities such as the DHS Office of the Chief Security Officer (OCSO) and the DHS Privacy Office.
- Ensure that remediation and all necessary coordination activities are completed before incident closure.
- Analyze incidents, identifying and notifying other stakeholders and DHS Components and Data Center SOCS that may be affected.
- Provide technical and investigative assistance to Components and Data Center SOCS.
- Provide technical and investigative assistance to the DHS Privacy Office as needed.
- Provide accurate and timely reports to the DHS CISO on significant incidents and on the status of DHS enterprise computer security.
- Develop and maintain an incident database that contains information on all discovered and reported incidents.
- Provide automated incident notification and reporting to senior DHS and Component leadership and stakeholders such as the DHS Privacy Office and the DHS OCSO, as well as external reporting entities such as US-CERT.
- Update US-CERT on incident status as required.
- Facilitate communications between DHS Components and Data Center SOCS (when applicable) for those incidents involving more than one Component (i.e., Master incidents).
- Provide ad hoc incident trending reports as requested by the DHS CISO.
- Oversee the department-wide vulnerability management program.

2.1.11 Component Security Operations Centers

Component SOCs are responsible for incident response, handling and reporting those incidents that pertain to the Component's network and data. In addition, Component SOCs are responsible for all network and host-based monitoring activities within the Component's network. This includes the detection, investigation, and subsequent reporting to DHS Enterprise SOC upon confirmation.

Component SOCs have functional, advisory, and reporting responsibilities in incident response that include the following:

- Focus security monitoring efforts on the Component network.
- Compile and maintain a list of mission-critical systems, financial systems, and applications. The list will assist in determining the classification of the Component's systems, and in prioritization of security incidents.
- Develop and publish internal computer security incident response plans and incident handling procedures, with copies provided to the DHS Enterprise SOC upon request.
- Investigate SENS and Incidents created by the DHS Enterprise SOC and comply with reporting timelines and escalation criteria outlined in Appendix F3, "Response Guidelines" to either escalate the SEN or close it.
- Monitor internal network enclave traffic (such as firewall logs and Network IDS) and host-based security events (e.g., audit logs, Host-based IDS/IPS). This includes workstation activity, internal server enclaves, Component-managed externally accessible applications and networks (e.g., DMZ, VPN), and applications hosted by third parties external to DHS.
- Request SEN escalation by the DHS Enterprise SOC, within the reporting timeframes and meeting the escalation criteria outlined in Appendix F3, "Response Guidelines."
- Conduct SEN and Incident investigation including traceback to the host.
- Request closure when a SEN has been identified as inconclusive or as a false positive after providing adequate explanation of investigational activities via EOConline.
- Respond to DHS ENTERPRISE SOC on SEN investigation activities based on the escalation criteria in Appendix F3, "Response Guidelines."
- Ensure 24x7 incident handling function exists for the Component.
- Lead the Component's information security incident handling and response activities, including identification, investigation, containment, eradication, and recovery. Coordinate information security incident response, investigation, and reporting to the DHS Enterprise SOC. Reporting should include all significant data such as the who, what, when, where, why, and how of a given information security incident. Coordinate information security incident handling activities with internal Component entities such as the Component Office of the Chief Security Officer, Component Privacy Office, and Internal Affairs.
- Collaborate with the Component Privacy Office, who is the lead, in privacy incident handling and response activities including identification, investigation, containment, eradication, and recovery. Assist Component Privacy Office in reporting to the privacy incident to the DHS

Enterprise SOC. Reporting should include all significant data such as the who, what, when, where, why, and how of a given privacy incident.

- Coordinate Component-level remediation efforts as mandated by DHS security policies and communicate remediation activity to DHS Enterprise SOC through EOConline log entries.
- Share applicable information Department-wide or Component-wide, for example by providing network and host-based indicators for malicious logic incidents; such sharing will facilitate implementation of proactive measures to prevent future incidents.
- Provide updates to the DHS Enterprise SOC for significant incidents every 24 hours.
- Request closure of incidents when Component SOC remediation and mitigation actions have concluded. Coordinate request for closure of privacy incidents with Component Privacy Office, who is the lead for privacy incident handling at the Component.
- Assist other Component SOCs with technical or investigation assistance as requested by the DHS Enterprise SOC.

2.2 Other Roles

Roles related to but not directly responsible for information system security are described in the subsections that follow.

2.2.1 Secretary of Homeland Security

The Secretary of Homeland Security is responsible for fulfilling the Department's mission, which includes ensuring that DHS information systems and their data are protected in accordance with Congressional and Presidential directives. The Secretary's role with respect to information system security is to allocate adequate resources.

To that end, the Secretary:

- Ensures that DHS implements its Information Security Program throughout the life cycle of each DHS system
- Submits the following to the Director, OMB:
    - The DHS CIO's assessment of the adequacy and effectiveness of the Department's information security procedures, practices, and FISMA compliance
    - The results of an annual independent information security program evaluation performed by the DHS Office of Inspector General (OIG)
    - The Senior Agency Official for Privacy's (SAOP) annual assessment of the Department's privacy policies, procedures, and practices
- Provides information security protection commensurate with the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the Department, and on information systems used or operated by the Department, or by a contractor or other organization on behalf of the Department
- Ensures that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the Department's operations

- Ensures that information security processes are integrated with strategic and operational planning processes to secure the Department's mission
- Ensures that the Department's senior officials have the necessary authority to secure the operations and assets under their control
- Delegates authority to the CIO to ensure compliance with applicable information security requirements

2.2.2 Under Secretaries and Heads of DHS Components

The Under Secretaries and Heads of DHS Components are responsible for oversight of their Components' information security program, including the appointment of CIOs. Undersecretaries and Heads of Components allocate adequate resources to information systems for information system security.

Under Secretaries and the Heads of DHS Components:

- Appoint CIOs
- Ensure that an Information Security Program is established and managed in accordance with DHS policy and implementation directives
- Ensure that the security of information systems is an integral part of the life cycle management process for all information systems developed and maintained within their Components
- Ensure that adequate funding for information security is provided for Component information systems and that adequate funding requirements are included for all information systems budgets
- Ensure that information system data are entered into the appropriate DHS Security Management Tools to support DHS information security oversight and FISMA reporting requirements
- Ensure that the requirements for an information security performance metrics program are implemented and the resulting data maintained and reported

2.2.3 DHS Chief Information Officer

The DHS CIO is the senior agency executive responsible for all DHS information systems and their security as well as for ensuring FISMA compliance.

The DHS CIO:

- Heads an office with the mission and resources to assist in ensuring Component compliance with the DHS Information Security Program
- Oversees the development and maintenance of a Department-wide information security program
- Appoints in writing a DHS employee to serve as the DHS CISO
- As appropriate, serves as or appoints in writing the AO for DHS enterprise information systems.

- Participates in developing DHS performance plans, including descriptions of the time periods and budget, staffing, and training resources required to implement the Department-wide security program
- Ensures that all information systems acquisition documents, including existing contracts, include appropriate information security requirements and comply with DHS information security policies
- Ensures that DHS security programs integrate fully into the DHS enterprise architecture and capital planning and investment control processes
- Ensures that System Owners understand and appropriately address risks, including interconnectivity with other programs and systems outside their control
- Reviews and evaluates the DHS Information Security Program annually
- Ensures that an information security performance metrics program is developed, implemented, and funded
- Reports to the DHS Under Secretary for Management on matters relating to the security of DHS systems
- Ensures compliance with applicable information security requirements
- Coordinates and advocates resources for enterprise security solutions
- Leads the DHS Contingency Planning program

2.2.4 Component Chief Information Officer

The Component CIO is responsible for Component information systems and their security as well as for ensuring FISMA compliance within the Component.

Component CIOs:

- Establish and oversee their Component information security programs
- Direct a review of the Component information security program plan be performed with a frequency depending on risk, but no less than annually
- Ensure that an AO has been appointed for every Component information system; serves as the AO for any information system for which no AO has been appointed or where a vacancy exists
- Ensure that information security concerns are addressed by Component Configuration Control Boards, Enterprise Architecture Board (EAB), and Acquisition Review Board (ARB)/Investment Review Board (IRB)
- Ensure that an accurate information systems inventory is established and maintained
- Ensure that all information systems acquisition documents, including existing contracts, include appropriate information security requirements and comply with DHS information security policies
- Ensure that System Owners understand and appropriately address risks, including risks arising from interconnectivity with other programs and systems outside their control

- Ensure that an information security performance metrics program is developed, implemented, and funded
- Advise the DHS CIO of any issues regarding infrastructure protection, vulnerabilities or the possibility of public concern
- Ensure that incidents are reported to the DHS SOC within reporting time requirements as defined in this Handbook's Attachment F, "Incident Response and Reporting."
- Work with the DHS CIO and Public Affairs Office in preparation for public release of security incident information. The DHS CIO, or designated representative, has sole responsibility for public release of security incident information.
- Ensure compliance with DHS information systems security policy
- Coordinate and advocate resources for information security enterprise solutions

CIOs of the following Components must appoint a CISO that reports directly to the Component CIO and ensures that the CISO has resources to assist with Component compliance with policy. CISOs must be DHS employees.

- CBP
- FEMA
- FLETC
- ICE
- TSA
- USCIS
- USCG
- USSS

CIOs of all other Components:

- Ensure that Component ISSMs have been appointed
- Provide the resources and qualified personnel to ensure Component compliance with DHS security policy

2.2.5 DHS Chief Security Officer

The DHS Chief Security Officer (CSO) implements and manages the DHS Security Program for DHS facilities and personnel.

The CSO is a senior agency official who reports directly to the Deputy Secretary on all matters pertaining to facility and personnel security within the DHS.

2.2.6 DHS Chief Privacy Officer

The DHS Chief Privacy Officer is the head of DHS Privacy Office and is responsible for establishing, overseeing the implementation of, and issuing guidance on DHS privacy policy. The DHS Chief Privacy Officer ensures that the Department's use of technology sustains, and does not erode, privacy protections relating to the collection, use, maintenance, disclosure,

deletion, and/or destruction of PII. The responsibilities of the DHS Chief Privacy Officer include oversight of all privacy activities within the Department, and ensuring compliance with privacy laws, regulations, and policies.

The DHS Chief Privacy Officer coordinates with the CIO and the CISO to provide guidance regarding information technology and technology-related programs and to develop and implement policies and procedures to safegaurd PII used or maintained by the Department in accordance with federal law and policy.

The DHS Chief Privacy Officer coordinates with Component Privacy Officers and Privacy PPOCs with policy compliance at the Component level.

The DHS Chief Privacy Officer, as the Department's Senior Agency Official for Privacy (SAOP):

- Develops, implements, and maintains a Department-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems
- Monitors federal privacy laws and policy for changes that affect the privacy program
- Allocates sufficient resources to implement and operate the Department-wide privacy program
- Develops a strategic Department privacy plan for implementing applicable privacy controls, policies, and procedures
- Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII
- Updates privacy plans, policies, and procedures biennially
- Oversees privacy incident management, including providing guidance to and, where appropriate coordinating with, components responding to suspected or confirmed privacy indidents
- Coordinates with the DHS CIO, DHS CISO, the DHS SOC, and senior management regarding privacy incidents
- Convenes and chairs privacy incident response teams, such as the Privacy Incident Response Team (PIRT) and the Core Management Group (CMG)
- Reviews and approves all Department Privacy Compliance Documentation, including PTAs, PIAs, and SORNs
- Designates Privacy Sensitive Systems as part of the Risk Management Framework based on approved PTAs. Privacy Sensitive Systems are those that maintain Personally Identifiable Information (PII)
- Ensures that the Department meets all reporting requirements mandated by Congress or OMB regarding DHS activities that involve PII or otherwise impact privacy
- Provides Department-wide annual and refresher privacy training

2.2.7 DHS Chief Financial Officer

The DHS Chief Financial Officer (CFO) implements and manages the DHS Financial Program, including oversight of DHS financial systems. The DHS CFO designates financial systems and oversees security control definitions for financial systems.

All systems on the CFO Designated Systems List are required to conform to the policies defined in Sections 3.5.1 and 3.15.

2.2.8 Program Managers

Program Managers ensure compliance with applicable Federal laws and DHS policy directives governing the security, operation, maintenance, and privacy protection of information systems, information, projects, and programs under their control.

Program Managers are responsible for program-level POA&Ms that may impact one or more systems.

2.2.9 System Owners

System Owners use Information Technology (IT) to help achieve the mission needs within their program area of responsibility. They are responsible for the successful operation of the information systems and programs within their program area and are ultimately accountable for their security. All systems require a System Owner designated in writing for proper administration of security.

2.2.10 Common Control Provider

The Common Control Provider is an organizational official responsible for planning, development, implementation, assessment, authorization, and maintenance of common controls.

2.2.11 DHS Employees, Contractors, and Others Working on Behalf of DHS

DHS employees, contractors, and others working on behalf of the DHS or its agencies are required by DHS Sensitive Systems Policy Directive 4300A to follow the appropriate set(s) of rules of behavior.

3.0 MANAGEMENT POLICIES

Management controls are security controls that focus on the management of risk and information system security. The controls include conducting risk assessments, developing Rules of Behavior, and ensuring that security is an integral part of both the System Engineering Life Cycle (SELC) and the Capital Planning and Investment Control (CPIC) processes. Management controls consist of techniques and concerns that are normally addressed by management personnel.

3.1 Basic Requirements

Basic security management principles must be followed in order to ensure the security of Department of Homeland Security (DHS) information resources. These principles are applicable throughout the Department and form the cornerstone of the DHS Information Security Program.

Component Chief Information Security Officers (CISO) and Information Systems Security Managers (ISSM) submit all security reports concerning DHS systems to the Component senior official or designated representative. Component CISOs/ISSMs interpret and manage DHS security policies and procedures to meet Federal, Departmental, and Component requirements. Component CISOs/ISSMs also answer data queries from the DHS CISO and develop and manage information security guidance and procedures unique to Component requirements.

Information Systems Security Officers (ISSO) are the primary points of contact for the information systems assigned to them. They develop and maintain Security Plans (SP) and are responsible for overall system security.

Refer to Section 2.0, Roles and Responsibilities for detailed information security requirements.

3.2 Capital Planning and Investment Control

Protecting computer systems, networks, and data is essential to effective management of information resources. Programs that have not met the standards and criteria may be denied funding.

Information security is a business driver and any risks found through security testing are ultimately business risks. Information security personnel should be involved to the maximum extent possible in all aspects of the acquisition process, including drafting contracts, and procurement documents. DHS Management Directive (MD) 102-01, “Acquisition Management Directive” and DHS MD 4200.1, “IT Capital Planning and Investment Control (CPIC) and Portfolio Management” provide additional information on these requirements. Consult the DHS CPIC Guide for more information.

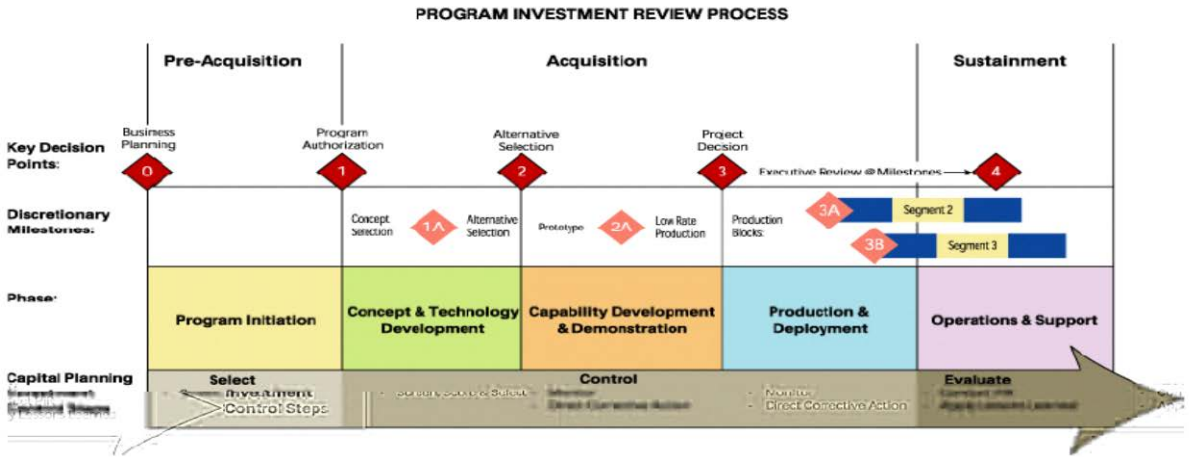
Two critical and complementary processes, CPIC and SELC govern information system management. Senior managers must ensure that information security is adequately addressed throughout all phases of systems engineering and investment lifecycles.

Department budgets must address the adequacy and effectiveness of information security policies, procedures, and practices. Security controls must be included in capital planning and procurement actions for both the current budget year and for the Future Years Homeland Security Program (FYHSP).

Capital Planning and Investment Control Responsibilities
DHS CIO Ensure that all information systems acquisition documents, including existing contracts, contain appropriate information security requirements and comply with DHS information security policies **Component CISOs/ISSMs** Manage information security resources including oversight and review of security requirements in funding documents **System Owners** Ensure that funding for implementation of information security is included in project life cycle planning **AOs** Ensure that funding for implementation of information security is included in project life cycle planning

3.2.1 Capital Planning and Investment Control Process

DHS investment management is governed by DHS Management Directive 1400, *Investment Review Process*. The Directive requires that all information systems investments be reviewed by the DHS Enterprise Architecture Board (EAB) at each key decision point (KDP). The security function has a formal role as a specialty reviewer, advising the EAB on whether the project should be allowed to proceed, based on how well security requirements are met at each lifecycle phase.



Process diagram illustrating how each KDP relates to its respective CPIC and SELC phase.

Program Authorization (KDP1) – Programs must demonstrate the results of operational analysis and identify requirements. With approval at KDP1, the initiative is:

- Designated as a Level 1 acquisition

- Directed to charter a major acquisition Integrated Product Team (IPT)
- Entered into the budget process (Typically the Fiscal Year +2 budget)
- Authorized to move to the Concept & Technology Development phase

Alternative Selection (KDP2) – Alternatives are evaluated for feasibility. Programs present their evaluations and basis for assessing relative merits. Promising solutions are defined in terms of:

- Cost
- Schedule
- Performance objectives
- Interoperability
- Supportability
- Infrastructure requirements
- Opportunities for tradeoffs
- Acquisition strategy
- Test and evaluation strategy, including Development Test and Evaluation (DT&E), and Operational Test and Evaluation (OT&E))

The Program Manager submits an updated Exhibit 300 based on these items; this information is used to monitor initiatives, direct corrective actions, and determine when the investment is ready to proceed to the Production and Deployment Phase.

Project Decision (KDP3) – The preferred alternative is reviewed for feasibility and refined prior to a full production commitment. The Program Manager reviews and updates documents prepared during previous phases, develops proposed exit criteria for the Production and Deployment Phase, and submits an updated Exhibit 300. This information is used to manage risks and determine when the investment is ready to proceed to the next phase. The future year's program plan must be fully funded. With approval at KDP 3, the investment is authorized to proceed to the Production and Deployment Phase.

Executive Review (KDP4) – Projects are reviewed against their performance and costs goals. Results of this review form the basis for decisions for project enhancement, re-engineering, or retirement.

3.3 Contractors and Outsourced Operations

Contractors fill a vital role in support of daily operations and share the responsibility to protect sensitive information. All personnel must adhere to the same standards.

All contract documents and statements of work incorporate information security requirements.

System Owners and Project Managers must review and include security requirements in solicitation documents *prior to the acquisition of information systems or services*. Information security must be a key factor in the source selection process and must be weighed against the sensitivity and criticality of the data to be processed. If the solicitation includes purchase of a

commercial off-the-shelf (COTS) application or if the system being developed has a COTS element, the security aspects of the COTS product must be considered.

Responsibilities for contractors and outsourced operations are provided in the following table.

Contractors and Outsourced Operations Responsibilities
Component CISOs/ISSMs
Establish and maintain a contractor and outsourced operations policy for the Component
System Owners/ Project Managers
Ensure that computer security requirements are reviewed and included in all applicable statements of work and other contractual agreements throughout the System Life Cycle
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 in other SELC documents, as required
ISSOs
Coordinate with the System Owners to ensure that contractor and outsourced operations policy requirements are met

All information security costs must appear in the initial investment management business case and in subsequent cost benefit analyses throughout the SELC. The system design and functional requirements documents must include computer security requirements.

3.4 Performance Measures and Metrics

The DHS CISO has developed a Department-wide security performance measures and metrics program. Appropriate information is included in this section.

Performance measures and metrics responsibilities are provided in the following table.

Performance Measures and Metrics Responsibilities
DHS CISO
Establishes an information security metrics program
Component CISOs/ISSMs
Define performance metrics to evaluate the effectiveness of the Information Security Program
Provide semiannual data to the CISO on their Component's progress in meeting DHS performance measures
ISSOs
Provide input to the identification and selection of specific performance metrics for their systems
Identify sources of metrics data and assign personnel to gather chosen data
Monitor metrics data collection and integrate/analyze data for reporting purposes

Performance Measures and Metrics Responsibilities
Provide performance metrics information to the Component CISOs/ISSMs as required

NIST SP 800-55, *Security Metrics Guide for Information Technology Systems* provides additional guidance on how organizations can, through the use of metrics, identify the adequacy of security controls, policies, and procedures, and describes an approach to assist management in determining where to best focus additional security resources.

A security metrics program includes four interdependent elements:

- Strong senior management support
- Practical security policies and procedures
- Quantifiable performance metrics
- Results-oriented metrics analysis

Metrics monitor the success of performance goals and objectives by quantifying the level of compliance of security controls.

Data required for calculating metrics must be easily obtainable, and the process under consideration must be measurable. To be measurable, a repeatable process is required. Only formal processes should be considered for measurement.

3.5 Continuity Planning for Critical DHS Assets

The Continuity Planning for Critical DHS Assets Program is vital to the success of the DHS Information Security Program. The Business Impact Assessment (BIA) is essential in the identification of critical DHS assets. Once critical systems are identified, continuity planning addresses the following two different but complementary elements:

- Continuity of Operations Planning (COOP)
- Contingency Planning (CP)

The COOP planning element requires Components to develop, test, exercise, and maintain comprehensive plans so that essential business functions can be continued. The COOP is business oriented and focuses on sustaining an organization's essential functions until the primary site can be restored.

The Contingency Planning element is designed to sustain and recover critical information services. Contingency plans focus on sustaining the critical applications and general support systems needed to support essential operations. The thrust of contingency planning is to assure the continuous availability of critical systems; to protect assets and vital records; to mitigate disruptions to operations; to provide maximum safety to personnel; and to achieve a timely and orderly recovery from a disruption to operations.

3.5.1 Continuity of Operations Planning

DHS must have the capability to ensure continuity of essential functions under all circumstances. COOP policies are designed to establish a Department-wide capability to react to emergency

events **(response)**; to restore essential business functions **(recovery)**; and to resume normal operations **(reconstitution)**.

COOPs focus on sustaining an organization's essential business functions at an alternate site until the primary site can be restored. This requires that Components develop, test, exercise, and maintain comprehensive plans to ensure that essential business functions can be continued following an emergency. Plans address three essential phases:

- Activation and Relocation (0-12 hours)
- Alternate Facility Operations (12 hours to Termination)
- Reconstitution (Termination to Return to Normal Operations)

General COOP planning responsibilities are provided in the following table.

Continuity of Operations Planning Responsibilities
DHS Continuity Planning Program Director
Administers the continuity planning for critical assets program
Develops, maintains, and promulgates program requirements
Provides oversight and ensures program compliance across DHS
Provides COOP guidelines to Components
Facilitates development and testing of COOP plans
Approves COOP plans and maintains COOP status
Component CISOs/ISSMs
Identify and align office functions with DHS essential functions
Identify vital records, information systems, and personnel requirements needed to recover office functions
Administer the Component Continuity Planning program
Ensure the development of the Component's COOPs
Ensure that COOPs are is implemented for each line of business
Provide COOP status and strategy to the DHS Continuity Planning Program Director
Develop and maintain a Component COOP Multi-Year Strategy and Program Plan
Component ISSOs
Comply with the Component COOP program
Perform continuity planning and testing and document results
Assist in development of the Component COOP Multi-Year Strategy and Program Plan
Ensure that operational security is maintained during any test or recovery activities

3.5.1.1 COOP Requirement

Components are required to develop, test, exercise, and maintain COOPs. COOPs are business oriented and focus on sustaining essential and supporting business functions at an alternate site for up to 30 days.

3.5.1.2 COOP Objectives

A COOP is designed to achieve the following objectives:

- Ensure the continuous performance of essential functions and operations during an emergency
- Protect equipment, vital records, and other assets to meet mission needs
- Reduce or mitigate disruptions to operations
- Reduce loss of life
- Minimize damage and losses
- Achieve a timely and orderly recovery from an emergency and resumption of full service to customers

3.5.1.3 COOP Plan Content

To facilitate their usefulness and acceptance, COOPs should be concise, and must address the following elements:

- Essential functions (including information systems requirements, vital records and databases, and functional recovery activities)
- Essential personnel
- Alternate operating facilities
- Interoperable communications
- Human capital issues (inclusion of occupant emergency planning)
- Devolution of control (delegations of authority and orders of succession)
- Reconstitution (return to normal operations)

COOPs normally focus on facility level and organization contingency planning. Information systems requirements, considered in terms of their support of essential and supporting office functions, should be documented in the COOP. Although contingency planning is a separate effort, these plans can be included in the COOP as appendixes. Close coordination with support operations is required to ensure availability at the alternate site(s).

3.5.1.4 COOP Test, Training, and Exercise

The most important aspect of a successful COOP is personnel training and periodic testing and exercising of the plan. Tests and exercises serve to validate specific aspects of plans, policies, procedures, systems, and facilities that would be used during an emergency and to identify weaknesses and correct them. Exercises and test results must be documented.

3.5.2 Contingency Planning

Contingency planning is an integral part of the Critical DHS Assets Program and is designed to ensure the availability of critical information systems under all circumstances. Components are required to develop, test, and maintain contingency plans.

Contingency planning is designed to establish a Department-wide capability to react to emergency events **(response);** to restore essential business functions if a disruption occurs **(recovery);** and to resume normal operations **(reconstitution)**. Plans focus on sustaining an organization's critical information services.

Contingency planning responsibilities are provided in the following table.

Contingency Planning Responsibilities
DHS Continuity Planning Program Director
Administers Continuity Planning for Critical DHS Assets Program.
Develops, maintains, and promulgates program requirements
Provides oversight and ensures program compliance across DHS Components
Provides contingency planning guidelines to Component CISOs/ISSMs
Facilitates the development and testing of Contingency Plans
Approves DHS Contingency Plans and maintains status
System/Network Administrators
Participate in all phases of the contingency planning process
Site Managers/System Owners
Ensure that the system's FIPS 199 potential impact for the availability security objective is correct and maintained to be consistent with system information processing changes
Ensure that adequate resources are budgeted for contingency planning, testing, and training consistent with the availability objective of the system
Ensure that adequate contingency plans are included in Security Authorization process documentation
Component CISOs/ISSMs
Establish Component continuity planning programs consistent with Department policy
Provide contingency planning status and strategy to the DHS Continuity Planning Program Director
Component ISSOs
Comply with the Component continuity planning program
Ensure that the system's FIPS 199 potential impact for the availability security objective is consistent with the information types processed, stored, and transmitted by the system
Ensure comprehensive contingency plans are developed, as required, for each major application and general support system under their purview
Perform contingency planning, testing/exercising, and training, as required.
Ensure operational security is maintained during any test or recovery activities

3.5.2.1 Contingency Planning Requirement

Requirements for implementation of contingency planning are found in

- NIST SP 800-34, Rev 1, "Contingency Planning Guide for Information Technology Systems," May, 1010

  NIST SP 800-34 considers continuity of support planning to be synonymous with contingency planning. Since a contingency plan is required for each major application and general support system, multiple plans may be maintained within the organization's COOP or Business Continuity Plan.

- Appendix III to OMB Circular A-130, "Management of Federal Information Resources," revised, November 30, 2000

  Appendix III requires development and maintenance of continuity of support plans.

- NIST SP 800-53, Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013, with updates as of January 15, 2014

- NIST SP 800-53 defines a family of security controls and identifies the level at which these controls should be developed for high, moderate, and low potential impact systems. DHS uses the FIPS 199 designation of the *availability* security objective (rather than the high water mark) to define the impact level applicable to contingency planning controls.

3.5.2.2 Contingency Plan Development

Contingency planning is designed to achieve the following objectives:

- Ensure the continuous availability of the critical information systems
- Protect assets and vital records needed to support mission needs
- Reduce or mitigate disruptions to operations
- Reduce loss of life
- Minimize damage and losses
- Achieve a timely and orderly recovery from an emergency and the resumption of full service to customers

3.5.2.3 Contingency Plan Format and Content

Contingency plans should be concise. Specific control requirements and levels of effort are determined based on the system's security categorization. The level of resources is based on the security categorization for the *availability* security objective.

Contingency plans must address the following elements for the potential level of impact on the system's *availability* security objective:

- Disruption impacts and allowable outage times
- Preventive controls and recovery strategies
- Vital records
- Responsible personnel

- Alternate operating facilities
- Devolution of control (delegations of authority and orders of succession)
- Reconstitution (return to normal operations)

3.5.2.4 Contingency Plan Test and Exercise

Testing the contingency plan identifies planning gaps. Tests and exercises serve to validate specific aspects of plans, policies, procedures, systems, and facilities to be used during an emergency. Both activities improve plan effectiveness and overall Department preparedness.

3.5.2.5 Contingency Plan Training

Training prepares recovery personnel for plan activation and improves plan effectiveness for overall Department preparedness. Appropriate personnel are to be trained in their contingency plan responsibilities according to the system's potential impact level of the *availability* security objective.

- High impact for availability – All personnel involved in contingency planning are to be identified and trained in the procedures and logistics of contingency planning and implementation, as well as in their roles and responsibilities in relation to contingencies. This training is to incorporate simulated events. Annual refresher training is to be provided.
- Moderate impact for availability – All system personnel involved in contingency planning are to be trained in the procedures and logistics of contingency planning and implementation, as well as in their roles and responsibilities in relation to contingencies. Annual refresher training is to be provided.
- Low impact for availability – Training is not required.

3.6 System Engineering Life Cycle

SELC methodology provides a structured approach to managing information systems projects. It also allows introduction of information security planning, including budgeting, review, and oversight. The SELC process begins when the Program Authorization decision of the CPIC process occurs.

Figure 2 shows the eight distinct phases in the SELC process.

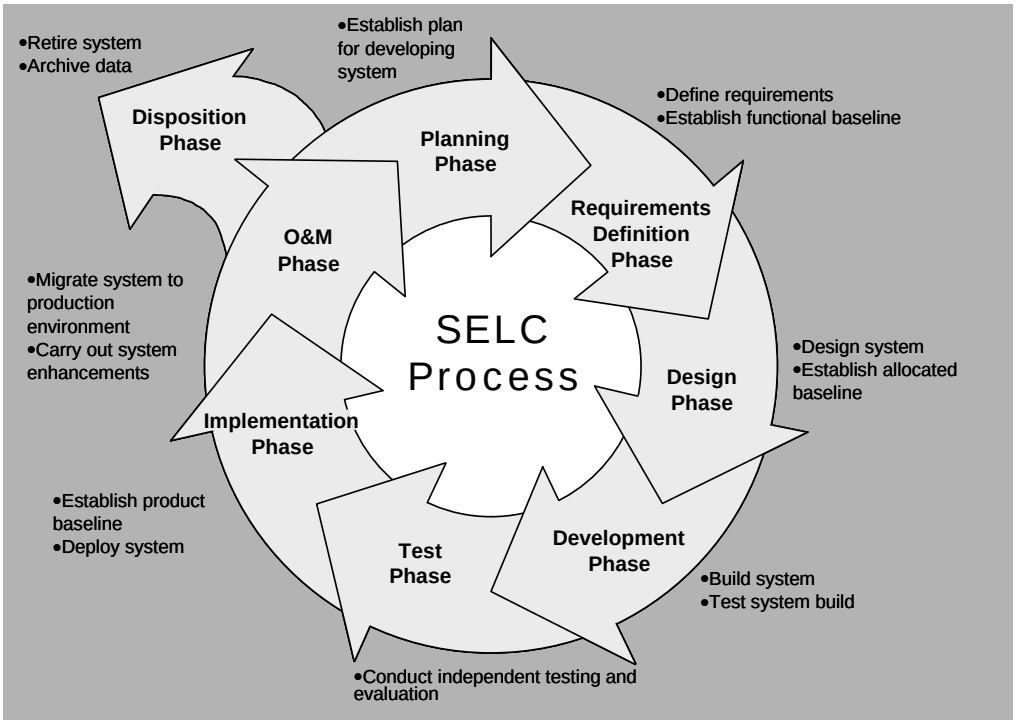


Figure 1 – The SELC process

SELC responsibilities are provided in the following table.

SELC Responsibilities
DHS CIO Defines and promulgates the SELC process Ensures that information security life cycle planning is integrated into capital planning and investment control processes **DHS CISO** Ensures that information security requirements are included in the SELC Oversees proper implementation of security controls in system development **Component CISOs/ISSMs** Establishes procedures for reviewing compliance with SELC documentation requirements Participates in capital planning and investment management meetings involving SELC considerations for systems and networks Ensures that required information security documentation is produced and reviewed in accordance with SELC milestones Approves information security documentation produced as part of the SELC process (except the

SELC Responsibilities
Security Authorization Process package)
ISSOs
Participates in planning and executing the SELC process
Provides information security expertise to system development teams
Reviews and comments on all SELC security documents
System Owners/Project Managers
Ensure required security documents and reviews are included in the SELC
Ensure that adequate funding is available for implementation of security requirements
Prepare required security documents

3.6.1 Planning

The Planning Phase defines the system concept from the user's perspective and establishes a comprehensive plan for developing the system. Information security activities include the following:

- Preparation of the initial Risk Assessment and Security Plan
- Ensuring that adequate budgetary resources for information security requirements are available

3.6.2 Requirements Definition

During the Requirements Definition Phase, users and technical staff define detailed requirements to ensure that the system will meet user requirements. This results in the establishment of a Functional Baseline. Information security activities include:

- Updating the Risk Assessment and Security Plan
- Reviewing Baseline Security Requirements
- Developing an initial Plan of Action and Milestones
- Developing an initial Security Test and Evaluation Plan
- Reviewing information security budget requirements
- Preparing the initial security inputs to the Training Plan
- Preparing the initial Contingency Plan

3.6.3 Design

The system development then moves to the Design Phase, during which the requirements are transformed into detailed design specifications. During the Design Phase, an Allocated Baseline is established and documented in the System Design Document. Information security activities include the following:

- Updating the Risk Assessment and Security Plan
- Reviewing budget requirements
- Developing Interconnection Security Agreements
- Updating the security information in the Training Plan
- Updating the Contingency Plan
- Preparing the initial Security Authorization Process package

3.6.4 Development

After formal approval of the design, the project enters the Development Phase. During this phase, the development team builds the system according to the design specified during the Design Phase and conducts development testing. The Development Phase represents an iterative process during which the development team builds the system, tests the system build, modifies the system based on any problems identified during Development Testing, and then tests the modified system build. Information security activities include the following:

- Conducting the initial Developmental Security Control Assessment
- Updating the Risk Assessment and Security Plan
- Developing the initial Operational Security Control Assessment
- Reviewing budget requirements
- Updating the Security Authorization Process package

3.6.5 Test

When the developed system is fully functional and has successfully passed Development Testing, the system development project moves into the Test Phase. During this phase, independent testing and evaluation is conducted to ensure that the developed system functions properly, satisfies the requirements (including security requirements) developed in the Requirements Definition Phase, and performs adequately in the host environment. Information security activities include:

- Conducting formal Developmental Security Control Assessment
- Reviewing budget requirements
- Updating the Risk Assessment and Security Plan
- Updating the Security Authorization Process package

3.6.6 Implementation

The system development project enters the Implementation Phase after the system has successfully passed testing and is ready for deployment. The output of this phase is the Product Baseline, which consists of the production system, databases, an updated data dictionary, associated infrastructure, and supporting documentation. During this phase the system is deployed to designated production sites. Information security activities include the following:

- Conducting the Operational Security Control Assessment on upgraded or new systems

- Reviewing adequacy of budget requirements
- Finalizing the security inputs in the Training Plans
- Updating the Risk Assessment and Security Plan
- Finalizing the Security Authorization package

3.6.7 Operations and Maintenance

After the system has been successfully deployed, it enters the Operations and Maintenance (O&M) Phase. During this phase, the system becomes operational and any necessary system modifications are identified and documented as "System Change Requests." These changes must be formally approved before they can be implemented. Information security activities include the following:

- Reviewing Security Authorization Process status and maintaining documentation currency
- Conducting annual user security awareness training and role-based training (e.g., training for ISSOs, AOs, network and system administrators, and managers)
- Maintaining adequate budgetary resources

3.6.8 Disposition

Finally, the system is retired from the operational environment during the Disposition Phase. Activities during this phase involve:

- Terminating system operations
- Removing the system from the production environment
- Archiving the system elements, data, and documentation
- Disposing of equipment and media in accordance with security requirements

3.7 Configuration Management

Configuration Management (CM) includes management of all hardware and software elements of information systems and networks. CM within DHS consists of a multi-layered structure – policy, procedures, processes, and compliance monitoring. Each Component uses its own appropriate level of configuration management.

CM applies to all systems, subsystems, and components of the DHS infrastructure, and ensures implementation and continuing life-cycle maintenance. CM begins with baselining of requirements documentation and ends with decommissioning of items no longer used for production or support.

The CM discipline applies to hardware, including power systems, software, firmware, documentation, test and support equipment, and spares. A Change Management Process ensures that documentation associated with an approved change to a DHS system is updated to reflect the appropriate baseline, including an analysis of any potential security implications. The initial configuration must be documented in detail and all subsequent changes must be controlled through a complete and robust CM process.

Configuration management has security implications in three areas:

- Ensuring that the configuration of subordinate information system elements is consistent with the Security Authorization Process requirements of the parent system
- Ensuring that any subsequent changes (including an analysis of any potential security implications) are approved
- Ensuring that all recommended and approved security patches are properly installed

As new systems and newly modified systems proceed through the SELC, changes must be documented and tested prior to placing the systems into an operational environment. The objective is to ensure that new vulnerabilities are not introduced during the change process. The same requirements apply to operational systems as they undergo periodic modifications.

In today's climate, new vulnerabilities quickly present themselves and often the risk of not implementing vendor-supplied patches exceeds the risk of installing an untested patch. Components must have provisions for reacting quickly as these critical patches are identified and released by the DHS Security Operations Center (SOC). Configuration management policies must include provisions for quickly testing and approving time-sensitive changes that result from newly released vulnerability information.

Configuration management responsibilities are provided in the following table.

Configuration Management Responsibilities
Component CISOs/ISSMs
Ensure that security issues are being addressed in configuration reviews and by Change Control Boards
Security Control Assessors
Re-assess the system if significant configuration changes have been made
AOs
Re-authorize systems if significant configuration changes have been made
Ensure that Project Managers and Development/O&M Support Teams implement an effective CM process in accordance with SELC requirements
Project Managers/ISSOs
Ensure that CM procedures are documented and implemented for all proposed configuration changes to information systems
Ensure that all proposed configuration changes to operating systems and applications are analyzed prior to implementation to determine if the proposed change has security implications
Maintain a capability to quickly approve and implement time-sensitive security patches in reaction to late-breaking security vulnerabilities identified by the DHS SOC
Ensure that all proposed configuration changes to operating systems, operating system security features, applications, critical system files, and system devices are formally approved, tested, and documented prior to the change being implemented
Ensure that all approved changes to the configuration baseline are documented, reviewed for accuracy, and that records are maintained for each system for both the current and all previous configurations

Configuration Management Responsibilities
Ensure that formal system configuration reviews are performed
Ensure that accurate system documentation and configuration logs are maintained to reflect current and prior configuration baselines
Prepare and distribute a CM plan for each system under their authority
Implement and enforce CM controls
Project Team
Understand and comply with the system CM plan
Comply with CM controls and procedures

Component CISOs/ISSMs, in cooperation with network operations leadership, determine when and how quickly late-breaking patches must be expedited through the CM process and installed on DHS systems.

The ISSO and Project Manager work with the appropriate development team (for new development systems) or the O&M Support Team (for fielded systems) to ensure that all proposed changes to the configuration baseline are analyzed and tested to determine their security implications. As new vulnerabilities are identified during the testing process, appropriate security software patches must be developed and installed prior to implementation of the proposed change. Any changes that impact the security posture of the system must be brought to the attention of the Security Control Assessor and the AO

Proposed configuration changes to operating systems, operating system security features, applications, critical system files, and system devices must be approved through the CM process and documented prior to the change being implemented. If the change is deemed to be significant, the Security Authorization Process documentation must be updated.

The CM process continues throughout the system life cycle.

3.8 Risk Management

Risk management is a process that allows System Owners to balance the operational and economic costs of protective measures to achieve gains in mission capability by protecting the information systems and data that support their organization's missions.

An effective risk management process is a vital element of a successful Information Security Program. An organization's risk management process is designed to protect the organization and its ability to perform its mission, not just its information system assets. The process identifies risks and assesses their impacts so that appropriate steps can be taken to reduce them to an acceptable level.

Effective risk management enables an organization to accomplish its mission(s) by:

- Better securing the information systems
- Enabling management to make well-informed risk management decisions
- Assisting management in authorizing information systems

Risk management responsibilities are provided in the following table.

Risk Management Responsibilities
DHS CISO
Establishes and enforces policy relating to the risk management process
Security Control Assessor
Evaluates the risk assessment document as part of the assessment process
Ensures that the risk assessment document contains information required for the Security Authorization Process
Informs the AO of the possible mitigation actions for residual risks
AOs
Determine the overall degree of acceptable risk based on the Component's mission requirements
Determine whether residual risks are within tolerable limits
Make a risk-based decision to grant a system Authority to Operate (ATO) or Interim Authority to Operate (IATO); or to deny system authorization because the risks are beyond an acceptable level
System Owners
Assist in determining the degree of acceptable residual risk based on the Department's mission requirements
Review the assessment package and ensure resources are provided to implement risk mitigation measures
Project Managers/ISSOs
Conduct the initial risk assessment
Ensure that the SP and risk assessment contain information required by assessment activities and address all appropriate management, operational, and technical controls
Initiate follow-on risk assessments if any significant changes to the system configuration or to the operational or threat environment have occurred, or every three (3) years, whichever comes first

Risk management is an integral part of the Security Authorization Process and contains three essential elements:

- Risk assessment
- Risk mitigation
- Evaluation and assessment

3.8.1 Risk Assessment

Risk assessments are used throughout a system's lifecycle to determine the extent of potential threats and risks. The results are used to identify appropriate security controls to reduce risks to an acceptable level.

There are nine major areas to consider when developing a risk assessment:

- System characterization
- Threat identification
- Vulnerability identification control analysis
- Likelihood determination
- Impact analysis
- Risk determination
- Control recommendations
- Results documentation

3.8.2 Risk Mitigation

Risk mitigation occurs after the risk assessment phase and encompasses the prioritization, evaluation, and implementation of appropriate security controls.

There are seven (7) major activities to be conducted as part of the risk mitigation phase:

- Prioritize actions
- Evaluate recommended control options
- Conduct a cost-benefit analysis
- Select appropriate controls
- Assign implementation responsibility
- Develop an implementation plan
- Implement selected controls

3.8.3 Evaluation and Assessment

Risk management is an ongoing process that will evolve as systems are updated and replaced. New risks can surface and risks previously mitigated can re-surface.

Components must conduct risk assessments whenever significant changes to the system configuration or to the operational or threat environment occur, or every three (3) years, whichever comes first. The risk assessment is a key element of the Security Authorization Process.

3.9 Security Authorization and Security Control Assessments

DHS periodically assesses the selection of security controls to determine their continued effectiveness in providing an appropriate level of protection.

It is recommended that Components pursue 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 consists 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 authorization and system risk assessment.

Detailed information for creating and managing POA&Ms is published in this Handbook's Attachment H, "Plan of Action and Milestones (POA&M) Process Guide."

The Federal Information Security Management Act (FISMA) directs that all Federal agencies develop and implement an agency-wide information system security program designed to safeguard information systems, assets, and data. The Department's Security Authorization Process policy is based on the recommendations set forth in NIST SP 800-37, and OMB Circular A-130.

Security Control Assessment is the comprehensive testing and evaluation of the management, operational, and technical security features of an information system. It 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.

Authorization is the official management decision that permits 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 an assessed system and officially grants Authority to Operate (ATO). AOs are to be identified in Information Assurance Compliance System (IACS). The Component CIO serves 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.

Components 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 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.

NIST SP 800-37 describes the six Risk Management Framework steps which are listed below:

- **Step 1 – Categorize Information System**
- **Step 2 – Select Security Controls**
- **Step 3 – Implement Security Controls**
- **Step 4 – Assess Security Controls**
- **Step 5 – Authorize Information System**
- **Step 6 – Monitor Security Controls**

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

The DHS Security Authorization Process is governed by the following NIST publications:

- NIST Special Publication 800-30, "Guide for Conducting Risk Assessments"
- NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems"
- NIST Special Publication 800-53, Rev. 4 "Recommended Security and Privacy Controls for Federal Information Systems and Organizations"
- NIST Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans"
- NIST Special Publication 800-59, "Guideline for Identifying an Information System as a National Security System"
- NIST Special Publication 800-60, Volume I: "Guide for Mapping Types of Information and Information Systems to Security Categories," and Volume II: "Appendixes to Guide for Mapping Types of Information and Information Systems to Security Categories"
- Federal Information Processing Standards Publication (FIPS Pub) 199, "Standards for Security Categorization of Federal Information and Information Systems"
- FIPS Pub 200, "Minimum Security Requirements for Federal Information and Information Systems

Assessment and Authorization responsibilities are provided in the following table.

Assessment and Authorization Responsibilities
DHS CISO
Establishes and enforces policy relating to the Security Authorization Process
Security Control Assessor

Assessment and Authorization Responsibilities
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
AOs
Determine degree of acceptable residual risk based on Department's mission requirements
Review the state of the security controls for the system and the Department's mission requirements
Assess the correctness and effectiveness of security controls and identify the level of residual risk for the system
Determine whether the residual risk is within tolerable limits
Make a risk-based decision to (1) grant system authorization, (2) grant an IATO for a designated period of time (no longer than 6 months - systems in development testing or prototypes only), or (3) deny system authorization.
System Owners
Assessment Responsibilities:
Ensure that adequate resources are budgeted for and allocated to the Security Authorization Process.
Review the results of the Initiation and Security Assessment phases and ensure that resources are provided to identify and implement risk mitigation measures.
Authorization Responsibilities:
Assist in determining degree of acceptable residual risk based on Department's mission requirements
Review the Assessment Package and ensure that resources are provided to implement risk mitigation measures
Project Managers/ISSOs
Ensure that the IACS tool is used to develop Security Authorization Process packages
Assessment Responsibilities:
Ensure that the Security Plan and Risk Assessment contain information required by assessment activities
Develop the Security Control Assessment plan, conduct the Security Control Assessment, and prepare the Security Control Assessment Report (the Security Assessment Report (SAR)).
Authorization Responsibilities:
Complete the final Risk Assessment, update the Security Plan, prepare the assessment findings, and prepare a Draft Assessment Statement.

Assessment and Authorization Responsibilities
Complete the Assessment Package and forward to the Security Control Assessor.
Maintain files of the Assessment Package.
Initiate re-authorization activities if any significant changes to the system configuration or to the operational/threat environment that might affect system security have occurred, or every three (3) years, whichever comes first.

3.9.1 Ongoing Authorization

The DHS OA Program builds upon an information system's existing Security Authorization; the purpose of the OA Program is continuous evaluation of security controls, based on system-specific information, and timely action in response to changes to information systems and risk posture.

Ongoing Authorization enhances the information assurance life cycle process by replacing the periodic three-year assessment cycle with ongoing security assessments that are driven by risk as opposed to time.

The DHS Ongoing Authorization Methodology describes detailed processes governing the Ongoing Authorization Program's requirements and entrance criteria for a Component and for a Component's systems. The OA Methodology defines the deliverables and templates required for maintaining compliance with Ongoing Authorization as well as required and recommended internal procedures.

3.9.1.1 Key Ongoing Authorization Artifacts

3.9.1.1.1 Control Allocation Table

The Control Allocation Table (CAT) is a risk-based tailoring of controls that outlines frequency, rigor, and impact of each control. It is updated over time to meet changing risks in response to triggers. Each system's security team determines how often each control was evaluated based on DHS 4300A guidance, NIST SP 800-53 tailoring guidance, accounting for mission, criticality and other organizational factors. The authoritative and accepted Control Allocation Table will be created and managed in IACS.

3.9.1.1.2 Trigger Accountability Log

The Trigger Accountability Log (TRAL) acts as a running list of all triggers for all systems in OA for each Component. The TRAL allows Components to track and document the number and type of events occurring for a system, provides DHS with visibility into Component activities, and serves as an audit trail.

The appropriate operational and security staff will constantly monitor for trigger events. Triggers can be either routine or non-routine. Routine triggers are events that are normal or scheduled occurrences. They are planned and are known to the operations and security personnel. Non-Routine triggers are events that are out-of-cycle, anomalies, of unknown origin or activity. They

are detected through Continuous Monitoring mechanisms (e.g. Intrusion Detection/Prevention Systems and Firewalls). These trigger types are explained in the table below.

Routine Triggers	Non-Routine Triggers
Minor system release	Security Incident –Pre-meditated Attack (External or Internal)
Major system release	Security Incident –Suspicious or Malicious User Activity (Internal or Remote) (Intentional or Unintentional)
Change in external connections	Zero Day Attack
Development/O&M contract turnover	Malware Introduction (Internal or External) (Malicious or Accidental)
System Owner change	
ISSO change	
Technology change (e.g. database)	

3.9.1.2 Component Admission

Components must meet the eligibility requirements and be approved by the Department to implement Ongoing Authorization. The criteria for Component eligibility are described in the subsequent sections.

3.9.1.2.1 Robust Continuous Monitoring

This requirement uses the DHS Scorecard, which is the barometer of Information Security Continuous Monitoring (ISCM) in DHS. The metric of the total ISCM score is the basis of this requirement. This average score is derived from the following ISCM Metrics:

- Hardware Asset Management
- Software Asset Management
- Configuration Management
- Vulnerability Management
- Anti–Virus
- Information Security Vulnerability Management (ISVM)

Maintaining an ISCM score of 80% or higher over three (3) consecutive months is indicative of a Component that has a fully functioning Continuous Monitoring initiative. Components interested in OA participation must meet that score.

3.9.1.2.2 Approved Common Controls

The Control Allocation Table (CAT) is a core requirement for systems to be admitted to OA. Components must define Common Controls within the IACS tool, along with expressed approval from the AO in the form of a signed Risk Acceptance letter. This ensures CATs are to be filled out accurately, showing the inheritance of controls from the Component CISO Program level.

3.9.1.2.3 Designated Ongoing Authorization Manager

The Component Ongoing Authorization Manager (OAM) will serve as the primary non-executive director of their OA Program. The OA Manager directs the Operational Risk Management Board (ORMB) and is the first line of defense for alerted triggers and communications from the Component CISO or the Department. At least one OAM must be designated in writing before a Component can be entered into the DHS OA Program. Components may opt to assign additional deputy OAM's at their discretion. Once a package has completed the necessary OA entrance requirements that are defined in official DHS policy documents (e.g., DHS 4300, OA Methodology), submission is then possible into the DHS OA Program.

3.9.1.2.4 Chartered Operational Risk Management Board

A key function of OA is the ORMB, which decides how triggers are handled and how risk is accepted or remediated. Each Component must determine how to operate or construct its ORMB, but it also must ensure ORMBs function as specified in the Ongoing Authorization Methodology and other DHS policies. While their membership and activities may have commonalities, the ORMB is different from the Change Management Board (CMB). Outlined below are activities that each board addresses.

Operational Risk Management Board (ORMB)	Change Management Board (CMB)
Activities that exceed risk threshold as defined in the Component's Risk Threshold Matrix (RTM)	Activities that do not exceed the risk threshold as defined in the Component's RTM
Events and anomalous activity that may impact security posture of the information system	Normal routine non-security-related activities involving changes to infrastructure configuration
Normal routine security-related changes that may have an impact on the security posture of the information system	Normal routine security-related changes that may have an impact on the security posture of the information system
Activities that may have an impact in the future, e.g. intelligence indicating increase threat level or knowledge of attack	CMB members may also be in the membership of the ORMB

3.9.1.2.5 System Admission Requirements

Components that have been approved for OA by DHS can nominate Systems to undergo OA. However, nominated Systems are not automatically enrolled in OA. Systems have their own eligibility criteria. The criteria for System eligibility are:

3.9.1.2.5.1 Component Accepted into the Ongoing Authorization Program

Systems that desire to be included in the Ongoing Authorization Program must have the oversight and management of a participating Component in order to process triggers, have a credible ORMB, and must enter all systems and all artifacts into IACS to ensure the system authorization of their individual programs.

3.9.1.2.5.2 Ongoing Authorization System Admission Letter

The Ongoing Authorization System Admission Letter serves as the formal CISO recommendation via the Authorizing Official (AO) of a system regarding its eligibility to begin participation in the DHS Ongoing Authorization (OA) program. This letter does not permit systems to be designated as an official OA system until a full review is performed by the DHS OA Team for suitability and subsequent admission.

3.9.1.2.5.3 Ongoing Authorization Recommendation Letter

The Ongoing Authorization Recommendation Letter serves as the formal CISO recommendation to the Authorizing Official (AO) of a system regarding triggers that get escalated from the ORMB and system eligibility to continue participation in the Ongoing Authorization (OA) program. This recommendation shall be completed and approved by all relevant parties as requested. DHS provides a template for the OA Recommendation Letter, but Components may develop their own internal communications as it relates to their unique mission and operations.

3.9.1.2.5.4 ATO Expiration Greater than 60 Days of Submission Date

Systems being considered for entrance into OA shall have an ATO within this time frame, unless by waiver of a Component CISO or AO. The logic behind this is that a system with an expiring ATO under the old system may not be up to date with its control assessments and evaluation of its security posture. It is ultimately up to the Components if they wish to accept this risk in writing and allow systems with ATOs of shorter expiration duration to enter OA. Systems that have expired ATOs are not permitted.

3.9.1.2.5.5 ISSO with Collateral Responsibilities that are less than 51%

Systems are required to have ISSOs with less than 51% of collateral duties in order to function within the limits of OA. The intent of this requirement is to ensure that systems have dedicated security professionals that have adequate time to execute the duties required as part of Ongoing Authorization

3.9.1.2.5.6 ISSO Trained on Ongoing Authorization Processes

ISSOs are required to have completed both Department and Component OA training to ensure that OA policies and procedures are carried out to maintain ongoing awareness of the security posture of DHS. This is in parallel with the current philosophy and requirements that are placed on Privileged Users in the DHS enterprise.

3.9.1.2.5.7 Approved Control Allocation Table (CAT)

Per DHS Ongoing Authorization (OA) entry criteria, each system must have a unique Control Allocation Table (CAT) that traces NIST controls to their proper source(s). The system's

security team will determine how often each control is evaluated based on NIST SP 800-53 tailoring guidance, mission, criticality and other organizational factors. After declaring how the system is to be monitored on an ongoing basis, internal and enterprise processes are used to maintain the system's security posture. Changes to the CAT may be necessary as events are triggered that affect the system.

To illustrate that all federal and organizational requirements are met, each of the system's controls are formally documented, numbered, and mapped to their source(s) in a CAT. By identifying controls and design requirements already tested (through inheritance, common controls, or through Continuous Diagnostics and Mitigation), the CAT provides insight into those controls NOT adequately assessed by an automated tool or other method. This information is combined with the system's mission and organizational objectives to determine the review frequency and impact for each control.

3.9.1.3 Information Assurance Compliance Systems (IACS)

Each system that participates in the DHS OA Program must utilize the IACS tool and ensure all information is accurate and up-to-date. During the migration from the Trusted Agent FISMA (TAF) system to IACS, all DHS systems in TAF and their stored artifacts were migrated to IACS. Each system is required to complete the IACS workflow up to the OA tasks. Systems cannot complete the OA portion of the IACS workflow until the previous tasks are completed.

The OA enrollment verification tasks in the IACS workflow are designed to prepare systems for entering and participating in the DHS OA Program. They also provide nonrepudiation for each level of the IACS approval process before the system is presented to the DHS OA Team for evaluation. The steps include filling out a checklist for the basic OA requirements and the subsequent approvals for the requirements which are illustrated in the figure below. These internal Component–based approvals of the requirements checklist, directly relate to the requirements for system entry into the OA Program, will help ensure a smooth evaluation process by the DHS OA Team.

Figure 4: IACS Ongoing Authorization Process Flow

Final approval and consideration of a system for OA remains with the DHS OA Managers. Once approved, a system must build the Control Allocation Table and complete the Ongoing Authorization System Admission Letter. Step-by-step procedures of how OA is implemented in IACS are available in the Appendix I: OA IACS Procedures.

3.9.2 FIPS 199 Categorization and the NIST SP 800-53 Controls

The *high watermark requirement* is the concept whereby the highest impact level of any of the security objectives (confidentiality, integrity, availability) must be used for a system as a whole. Within DHS, the high water mark requirement is amplified to reflect the actual security requirements that controls must meet.

Within DHS, controls required to support the security objectives for an information system are implemented. There is no requirement to implement extra controls beyond this minimum standard, but any program may implement additional or more stringent controls. This policy amplification is a Department-level risk-based decision that is consistent with the FISMA

requirement to "cost-effectively reduce information security risks to an acceptable level." The tailoring of controls and use of compensating controls is also consistent with providing the safeguards necessary to reduce the risks within a specific operating environment.

This policy amplification is also consistent with the NIST information security guidance which promulgates the "concept of risk-based decisions." The due diligence required by FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," requires determination of the exact impact level of each type of information on the system, and on each of the security objectives; this due diligence will lead to well-defined impact levels for confidentiality, integrity, and availability across systems. It is important, when using a risk-based decision, to minimize the security controls and to ensure that all of the information and the risks to that information are clearly defined and documented, so that the AO can make an informed risk-based decision for the system and its information in its specific operational environment.

The "*DHS FIPS 199 Workbook*" defines impact level categories (high, moderate, low). Each security objective is assigned to one of these categories. Appropriate control implementation is given by the *Workbook* for each category; for example, a system with low risk availability, high risk integrity, and low risk confidentiality is not required to implement high controls across the board, but rather the controls that revealed by the analysis. In this example, categorization analysis would indicate high level integrity controls and low level controls confidentiality and availability.

For systems involving Personally Identifiable Information (PII), the confidentiality security objective is assigned a minimum impact level of "moderate." If warranted by a risk-based assessment the confidentiality security objective is elevated to "high."

All CFO Designated Systems are assigned a minimum impact level of "moderate" for confidentiality, integrity, and availability. If warranted by a risk based assessment, the integrity objective is elevated to "high."

This Handbook's Attachment M, "Tailoring the NIST SP 800-53 Security Controls," lists the NIST SP 800-53 controls by impact level and by security objective, and provides information on the possible tailoring of these controls and the use of compensating controls.

3.9.3 Privacy Assessment

Information systems that collect, use, maintain, or disseminate PII are required to complete privacy compliance documentation. To determine whether a system is a Privacy Sensitive System (see Section 1.4.18), all System Owners must submit a Privacy Threshold Analysis (PTA) to the DHS Privacy Office for review. See Section 3.14, Privacy and Data Security for additional information.

As part of the Security Authorization Process, the confidentiality security objective for all Privacy Sensitive Systems is assigned an impact level of at least moderate.

3.9.4 E-Authentication

E-Authentication security requirements apply to information systems that allow online transactions. For systems where e-authentication security requirements apply, two additional steps are required:

- Determine the potential impact of authentication errors
- Determine the required assurance level for authentication

The E-Authentication Workbook and instructions are available on the DHS CISO Web page. The DHS Compliance Help Desk (202) 343-2500 can also provide assistance in obtaining these documents.

3.9.5 Risk Assessment

Risk Assessment is the process of identifying risks to system security, determining the probability of occurrence and the resulting impact, and identifying additional safeguards that would mitigate that impact. An initial risk assessment is used to understand the unique system risks and to determine whether or not any controls are required to address specific threats or weaknesses. The initial assessment incorporates system characterization information, security categorization, PTA and PIA, and e-Authentication assessment. The results are used to directly address the controls that will be documented in the Security Plan and implemented in the system.

An initial Risk Assessment is conducted within IACS whenever a Security Authorization Process package is initiated.

The initial assessment is created after security controls are implemented and tested, and is updated and revised whenever corrective actions or changes are applied. The amount of residual risk is identified throughout the process.

DHS follows the overall risk process as described in NIST Special Publication 800-30, Guide for Conducting Risk Assessments."

The *Security Authorization Process Guide* published by the DHS Office of the Chief Information Security Officer provides detailed information on developing Risk Assessments.

3.9.6 Security Plan

The SP provides a complete description of an information system, including purposes, functions, system boundaries, architecture, user groups, interconnections, hardware, software, encryption techniques, transmissions, and network configuration. It also provides an overview of the system's security requirements, describes the controls in place or planned, and delineates the responsibilities and expected behavior of all individuals who access the system. The SP, typically written in conjunction with the Risk Assessment, is refined throughout the authorization process.

An SP template is provided in RMS. The template and the RMS Requirements Traceability Matrix (RTM) provide a basic structure to ensure consistency and completeness within the document. The DHS *Security Authorization Process Guidance for SBU Systems: Users Manual* provides detailed information on completing the SP within RMS.

3.9.7 Contingency Plan

A Contingency Plan documents the management policies and procedures designed to maintain or restore business operations in the event of emergencies, system failures, or disaster. Specific control requirements and level of effort are determined based on the system's security categorization. The level of resources for the Contingency Plan is based on the security categorization for the availability security objective:

- For systems with a **low impact for availability**, the System Owner may determine the Contingency Plan format and content that is appropriate for the system and its environment. The Contingency Plan created in IACS is used for tailoring contingency plans.
- For systems with a **moderate impact level for availability**, the default Contingency Plan in IACS is used.
- For systems with a **high impact level for availability** a rigorous Contingency Plan is developed. The DHS-developed high impact contingency plan, "IT Contingency and Disaster Recovery Plan," is be used; it is found in IACS and conforms to the template in this Handbook'**s** Attachment K, "IT Contingency Plan Template."

The DHS "Security Authorization Process Guide" provides detailed information on developing the Contingency Plan using IACS.

3.9.8 Security Control Assessment Plan

The RTM is generated by IACS as part of the Security Authorization Process package; it is populated with sample test procedures. The procedures will need to be tailored to the particular SP, risks, and system environment, and they will need to be supplemented with detailed technical methods and procedures.

The complete Security Control Assessment Plan includes the primary document and any supporting material. Typically, supporting material includes the documented test procedures contained in the IACS RTM.

The DHS *Security Authorization Process Guide* provides detailed information on using IACS to develop the Security Control Assessment Plan. Once the Risk Assessment, SP, and Security Control Assessment Plan are completed and approved by the System Owner and agreed to with the Security Control Assessor, Security Control Assessment testing can be conducted as part of the assessment process. Results of the testing are documented in the Security Assessment Report.

3.9.9 Contingency Plan Testing

Contingency Plan testing is the process of simulating an information security event and the subsequent activities undertaken to restore and recover the system.

Contingency Plan testing is required only for systems with a moderate or high impact for the availability security objective; it is optional for systems with a low impact for availability. Testing requirements are provided in the following sections.

3.9.9.1 Systems with High Impact Availability — *Testing Required*

High Impact Availability systems require an established alternate site as part of their Contingency Plans, and resources for establishing an alternate site must be identified and made available.

Annual Contingency Plan testing is required; a full-scale test is preferred; in a full-scale test, the triggering incident is simulated, but the detection, containment, and recovery steps is executed in accordance with and by the actual individuals listed in the plan. This test includes coordination with and involvement of alternate site personnel, and has the following objectives:

1. Demonstrate that the system(s) can be brought to operational condition(s) at the designated alternate site by following the procedures and instructions described in the plan.
2. Verify that the Contingency Plan can be accomplished with resources located away from the site where the incident occurred.
3. Verify that the organizational units responsible for the Contingency Plan fully understand and are able to execute their responsibilities in a timely manner.
4. Verify that the system(s) can be brought to an operational condition within the allotted recovery time.
5. Verify that system information can be restored to the expected state, so that operations can resume in a synchronized manner.
6. Verify that authorized personnel are able to access information on restored systems and that connectivity can be re-established.

A rigorous tabletop exercise, with a planned follow-on for a full-scale test, may be conducted whenever circumstances preclude a full-scale test. The tabletop exercise is described below in the following section on moderate impact systems.

3.9.9.2 Systems with Moderate Impact for Availability — *Testing Required*

Moderate Impact Availability systems should have an alternate site identified as part of their Contingency Plans, and resources for establishing an alternate site should be identified and made available, a full-scale test of the Contingency Plan.

Annual Contingency Plan testing is required and a full-scale test is encouraged, but is not required. A tabletop exercise is acceptable under most circumstances for most moderate impact systems, as determined by the System Owner. In a tabletop exercise, the triggering incident, detection, containment, and recovery are simulated and a walk though is conducted by using a prepared scenario to demonstrate how system recovery would be achieved. Recovery steps are executed in accordance with and by the actual individuals listed in the plan. This test includes coordination with and involvement of the alternate site personnel, demonstrating that:

- Results for each step are being simulated as rigorously as possible.
- There is reference only to only personnel and other resources that will be located away from the site where the incident occurs.
- The exercise requires each organizational unit to explain how they would carry out their responsibilities.

- There is a timeline, with reasonable times for events, used to illustrate that the system could be brought to an operational condition within the allotted system recovery time.
- The exercise illustrates how access to system information by authorized business area personnel would be reestablished.

3.9.9.3 Systems with Low Impact for Availability — *Testing Optional*

Contingency Plan testing is optional for systems whose with low impact for availability. At a minimum, the plan is reviewed and evaluated for feasibility every two years or whenever significant changes are made. A memo is developed that indicates that "the system is a FIPS 199 low availability impact system; therefore, the system's and that the Contingency Plan is not required to be tested is included as part of the system description in the SP."

3.9.10 Security Assessment Report

The Security Assessment Report (SAR) summarizes the results of the Security Control Assessment and indicates the system's level of compliance with the security controls defined in its SP. Residual risks are also documented. Security Control Assessment results are attached to support the findings in the SAR.

3.9.11 A SAR is automatically created in IACS. Plan of Action and Milestones

A Plan of Actions and Milestones (POA&M) is required as part of the authorization package. The POA&M documents any the weaknesses that will be mitigated and the corrective actions that must be taken. The POA&M It details the resources required, milestones, and scheduled completion dates, and assigns actions to individuals. Detailed guidance on the POA&M process is found in Attachment H to this Handbook, Plan of Action and Milestones (POA&M) Process Guide. When reviewing the authorization package, the AO may stipulate that certain POA&M activities be completed within a specific timeframe, or that additional compensating controls be implemented as a condition for authorization.

3.9.12 Authorization to Operate Letter

Authorization to Operate (ATO) or Denial of Authorization to Operate letters are generated based on the appropriate AO's decision after reviewing the authorization package. The package includes the following documents:

- Security Plan (SP)
- Security Assessment Report (SAR)
- Plan of Action and Milestones (POA&M)
- Security Control Assessor Transmittal Letter (documents the Security Control Assessor's recommendation (i.e., Authorization to Operate or Denial to Operate)
- Any supplemental information requested by the AO or Security Control Assessor (e.g., Contingency Plan, final Risk Assessment, Configuration Management Plan, Standard Operating Procedures, Concept of Operations)

For operational systems, the AO makes a risk-based decision either to grant full ATO or deny authorization to operate. Authorizations to operate systems may be granted for a maximum of three (3) years. Should Components require a system to operate in a production environment for six (6) months or less an ATO authorization period waiver from the DHS CISO is required.

3.9.13 Interim Authorization to Operate

An Interim Authorization to Operate (IATO) provides a limited authorization to operate development, testing, or prototype systems under specified terms and conditions and acknowledges greater risk to the organization's operations and assets. An AO may grant one (1) six (6) month IATO, and may extend this period for an aditional six (6) monthsThe AO may grant an IATO for development, testing, or prototype systems. IATOs may not be used for production systems under any circumstances. An IATO provides a limited authorization to operate the system under specified terms and conditions and acknowledges greater risk to the organization's operations and assets. A system operating with an IATO is undergoing development testing or a prototype system is not considered authorized during the IATO period.

The AO must sign a formal ATO letter subsequent to Key Decision Point 3 of the life cycle development. The DHS Security Authorization Process Guidance for SBU Systems: Users Manual provides detailed information on the authorization phase and on the ATO letter.

The AO must sign a formal ATO letter subsequent to Key Decision Point 3 of the life cycle development. The DHS *Security Authorization Process Guide* provides detailed information on the authorization phase and on the ATO letter.

Decision	Criteria
Authorization to Operate (ATO)	The AO accepts the residual risk to the Department's operations or assets after assessing the results of the security assessment. A full ATO is issued and the system is authorized without any significant restrictions or limitations on its operation.
Interim Authorization to Operate (IATO) (for systems in development testing and prototype systems only)	The AO may issue an IATO for systems in development testing or for prototype systems after assessing the results of the security assessment. The IATO authorizes the system to operate for up to six (6) months. During this period, the effectiveness of security controls must be closely monitored. If the AO has not officially authorized the system by the end of the IATO, he or she may grant a second and final IATO for a period of up to six (6) additional months. The information system must receive a full ATO prior to becoming operational.
Denial of Authorization to Operate	Whenever the AO finds that the residual risk to the Department's operations or assets is unacceptable, the authorization to operate the system is denied. The system is not authorized and cannot be placed into operation. For a system currently in operation, all activity is halted.

3.9.14 Annual Self-Assessments

Annual assessments are performed during the Continuous Monitoring Phase of the authorization. They provide ongoing oversight and monitoring of the system's security controls and serve to inform the authorizing official whenever changes occur that may impact the security of the system. During this phase, the system's status is monitored to ensure that residual risk is kept within the acceptable level, and that any significant changes to the system configuration or

operational or threat environment are identified. Components must re-authorize their systems every three (3) years or whenever a major change occurs.

The automated reporting tool IACS addresses the annual self-assessments.

3.10 Information Security Review and Assistance

FISMA requires a thorough annual review of the DHS Information Security Program. This review must include a report on the degree to which security requirements have been implemented, significant deficiencies discovered, remedial actions that have been taken or are in progress to correct deficiencies, and level of compliance with NIST standards. This Handbook's Attachment E, "FISMA Reporting," provides detailed information on FISMA reporting.

Information security review and assistance responsibilities are provided in the following table.

Information Security Review and Assistance Responsibilities
DHS CIO
Designates a full-time CISO
Prepares the annual Congressional information security compliance report as required by FISMA
DHS CISO
Coordinates and prepares for the annual DHS Inspector General review of the Information Security Program
Reviews and approves all DHS information security policies
Establishes and implements an Information Security Review and Assistance Program
Prepares and distributes a review and assistance handbook based on applicable NIST guidance
DHS Compliance and Oversight Program Director
Develops and implements a compliance review and assistance program
Component CISOs/ISSMs
Implement an Information Security Review and Assistance Program at the Component level
Schedule information security review and assistance visits and ensure that these visits are completed
Provide trained personnel to participate in review and assistance visits
Coordinate with ISSOs and provide guidance and oversight in identifying and documenting deficiencies and prioritizing them based on missions, risk, and funding
Review and monitor POA&Ms
Ensure that POA&M updates to IACS are timely (i.e., by March 10, June 10, September 15, and December 10 annually)
Coordinate issues with the Compliance and Oversight Program Director
Generate candidate information security policies, as the need arises, for CISO review and approval
Review NIST and other directives for applicability to the DHS Information Security Program
ISSOs

Information Security Review and Assistance Responsibilities
Prepare security self-assessment documentation as directed by the Component CISO/ISSM
Identify personnel qualified to participate in review and assistance visits
System Owners
Ensure that ISSOs have access to resources adequate for conducting self-assessments and review and assistance visits
Implement corrective actions for deficiencies found during self-assessments
Site Managers
Ensure that adequate personnel resources are available to participate in site assistance visits

3.10.1 Review and Assistance Management and Oversight

Senior management participation is necessary for the successful implementation and management of the Information Security Program. The scope and complexity of the requirements requires active participation and oversight by a senior DHS official with a staff of qualified security professionals. The DHS CISO serves as the senior manager who reviews and approves information security policy, oversees the information security assistance program, and prepares the annual assessment report.

3.10.2 Information Security Assistance

Components must provide on-site assistance to their organizations to the maximum extent practicable, in accordance with the Information Security Review and Assistance Program. Component CISOs/ISSMs coordinate with ISSOs and provide guidance and oversight in identifying deficiencies and prioritizing them based on missions, risk, and funding. The size and geographic dispersion of DHS offices and organizations require close coordination and collaborative planning between the DHS CISO, Component CISOs/ISSMs, and ISSOs. Active support by site personnel and system development teams is imperative for the success of the assistance program.

3.10.3 Information Security Reviews

Information security controls are specified in accordance with FIPS 200 and NIST SP 800-53; NIST SP 800-53A is used for assessment of security control effectiveness and for annual FISMA reporting. System and site ISSOs have primary responsibility for completing the annual review and reporting results to senior management in accordance with the procedures established by the Component CISO/ISSM. The Component CISO/ISSM monitors ISSO performance, provides updates to the IACS database, and interacts with the DHS Compliance and Oversight Program Director.

3.11 Security Working Groups and Forums

Working groups and other forums representing various functional areas convene on a regular basis.

3.11.1 CISO Council

The CISO Council is the management team responsible for developing and implementing the DHS Information Security Program. The Council is responsible for implementing a security program that meets DHS mission requirements, and also for reviewing specific topic areas assigned by the DHS CIO or the DHS CISO.

The CISO Council is also responsible for establishing and implementing significant security responsibilities; promoting communications between security programs; implementing information systems security acquisition requirements; and developing security best practices in all enterprise and Component information security programs.

Note: Periodically, the CISO Council may be convened to include Component ISSMs.

3.11.2 DHS Information Security Training Working Group

The DHS Information Security Training Working Group is established to promote collaboration on information security training efforts throughout the Department and to share information on Component-developed training activities, methods, and tools, thereby reducing costs and avoiding duplication of effort. The Information Security Training Working Group is chaired by the DHS Program Director for Information Security Training.

3.11.3 DHS Security Policy Working Group

The DHS Information Security Policy Director chairs or appoints the chair for the Security Policy Working Group. The DHS Security Policy Working Group is established to promote collaboration involving all Components in the maintenance of DHS information security policy.

3.11.4 DHS Enterprise Services Security Working Group

The DHS Enterprise Services Security Working Group is established to ensure the development, review and vetting of proposed security documents for current and proposed enterprise service solutions and service offerings. It also provides recommendations to the CISO Council for review and approval. The Enterprise Services Security Working Group is chaired by the DHS CISO, the DHS Headquarters CISO, and Executive Director of Enterprise Systems Development Office or their delegates.

3.12 Information Security Policy Violation and Disciplinary Action

Individual accountability is a cornerstone of an effective security policy. Component Heads are responsible for taking corrective actions whenever security incidents or violations occur and for holding personnel accountable for intentional violations. Each Component determines how to best address each individual case.

Information security violations may result in disclosure of sensitive information to unauthorized individuals; unauthorized modification or destruction of data; loss of processing capability; or loss or theft of system resources. Violations also include failure to adhere to DHS policy regarding appropriate use of Departmental computer resources. The DHS SOC initiates necessary investigations and notifies appropriate law enforcement authorities, who pursue the investigation and recommend disciplinary action, if required.

Information security policy violation and disciplinary action responsibilities are provided in the following table.

Information Security Policy Violation and Disciplinary Action Responsibilities
Users
Be aware of information security policies described in this Handbook and in other references provided by DHS security officials
Be aware of and understand the disciplinary actions associated with violations of information security policy

3.13 Required Reporting

FISMA requires that the status of the DHS Information Security Program be reported to the OMB on a recurring basis.

The DHS CISO submits quarterly reports and an annual summary report to OMB. Components update status information on a continual basis using the IACS reporting tool. The status information is collected and compiled for FISMA and other status reports. For additional information, see this Handbook's Attachment E, "FISMA Reporting," and Attachment H, "Plan of Action and Milestones (POA&M) Process Guide."

Components use IACS when reporting Information Security Program status.

FISMA reporting responsibilities are provided in the following table.

FISMA Reporting Responsibilities
DHS Chief Privacy Officer
Completes the Section D: Senior Agency Official for Privacy section of the FISMA report
Completes any additional privacy artifacts required for the FISMA report
Reviews, and if appropriate approves, compliance with all privacy controls
Component CISO/ISSM/ISSO
Ensure that the IACS automated tool is used for required reporting
Ensure that Security Authorization Process artifacts (e.g., Privacy Impact Assessment, Security Plan, Security Test & Evaluation Report, Contingency Plan Test Results, Risk Assessment, ATO letter) are uploaded into IACS.

3.14 Privacy and Data Security

The DHS Privacy Office is responsible for privacy compliance across the Department, including assuring that technologies used by the Department sustain and do not erode privacy protections relating to the use of personal and Departmental information. The DHS Chief Privacy Officer has exclusive jurisdiction over the development of policy relating to Personally Identifiable Information (PII) and to privacy-sensitive programs, systems, or initiatives. Questions concerning privacy-related policy should be directed to the Component Privacy Office or Privacy Point of Contact (PPOC). If the Component does not have a Privacy Office or PPOC, then please contact the DHS Privacy Office (privacy@hq.dhs.gov or 202-343-1717) or refer to the DHS Chief Privacy Officer Web page at www.dhs.gov/privacy for additional information.

The privacy controls in NIST SP 800-53 Rev 4, Appendix J, are primarily for use by an organization's Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) when working with program managers, mission/business owners, information owners/stewards, Chief Information Officers, Chief Information Security Officers, information system developers/integrators, and risk executives to incorporate effective privacy protections and practices (i.e., privacy controls) within organizational programs and information systems and the environments in which they operate. The privacy controls facilitate DHS efforts to comply with privacy requirements affecting those Department-wide and Component programs and systems that collect, use, maintain, share, or dispose of PII or other activities that raise privacy risks. While the security controls in Appendix F are allocated to the low, moderate, and high baselines in Appendix D, the privacy controls in Appendix J are selected and implemented based on DHS' privacy requirements and the need to protect the PII of individuals collected and maintained by DHS information systems and programs, in accordance with federal privacy legislation, policies, directives, regulations, guidelines, and best practices.

3.14.1 Personally Identifiable Information

Various regulations place restrictions on the Government's collection, use, maintenance, and release of information about individuals. Regulations require agencies to protect PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or Department employee or contractor.

Sensitive PII is PII which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of Sensitive PII include Social Security numbers, Alien Registration Numbers (A-number), medical information, and criminal history. The sensitivity of this data requires that stricter handling guidelines be applied. For more information on handling Sensitive PII see: *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security.*

Consistent with the DHS *Fair Information Practice Principles (FIPPS)*, PII collected and maintained by DHS should be accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices. In addition, DHS adheres to data minimization and retention requirements to collect, use, and retain only PII that is relevant and necessary for the

purpose for which it was originally collected. Programs will retain PII for only as long as necessary to fulfill the purpose(s) specified in public notices and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule.

Additional PII and Sensitive PII-related policies are included in the following sections of the DHS 4300A *Sensitive Systems Handbook*.

- Section 3.9, Security Authorization Process, and Security Control Assessments – For Privacy Sensitive Systems, the confidentiality security objective is assigned an impact level of at least moderate.
- Section 4.8.2, Laptop Computers and Other Mobile Computing Devices – All information stored on any laptop computer or other mobile computing device is to be encrypted using mechanisms that comply with Section 5.5, Encryption, of this policy.
- Section 5.2.2, Automatic Session Termination – Sessions on workstations and on laptop computers and other mobile computing devices are to be terminated after twenty (20) minutes of inactivity.
- Section 5.3, Auditing – DHS defines computer-readable data extracts as "any Federal record or collection of records containing sensitive PII that is retrieved from a DHS-owned database, through a query, reporting tool, extract generation tool, or other means that is then saved into removable media and/or a separate computer-readable device or application such as another database, a spreadsheet, or a text file." (Attachment S1, *DHS 4300A Sensitive Systems Handbook*).
- Section 5.4.1, Remote Access and Dial-in – Remote access of PII must be approved by the AO. Strong authentication via virtual private network (VPN) or equivalent encryption (e.g., https) and two-factor authentication is required. DHS 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. Restrictions are placed on the downloading and remote storage of PII accessed remotely, as noted below in this document.
- Attachment S, "Compliance Framework for Privacy Systems.

The DHS Privacy Office works with Component Privacy Officers, PPOCs, Program Managers, System Owners, and information systems security personnel to ensure that sound privacy practices and controls are integrated into the Department's operations. The DHS Privacy Office implements three types of documents for managing privacy practices and controls for information systems:

- A PTA provides a high level description of an information system including the information it contains and how it is used. The PTA is used to determine and document whether or not a PIA and/or SORN are required.
- A Privacy Impact Assessment (PIA) is a publicly released assessment of the privacy impact of an information system and includes an analysis of the PII that is collected, stored, and shared.

- A System of Records Notice (SORN) describes the categories of records within a system of records and describes the routine uses of the data and how individuals can gain access to records and correct errors.

To promote privacy compliance within the Department, the Office has published official Department guidance regarding the requirements and content for PTAs, PIAs, and SORNs. Privacy Compliance Guidance can be found on the DHS Privacy Office website at www.dhs.gov/privacy.

3.14.2 Privacy Threshold Analyses

The PTA provides a high-level description of the system, including the information it contains and how it is used. PTAs are required whenever a new information system is being developed or an existing system is significantly modified. System Owners and Program Managers are responsible for writing the PTA as part of the SELC process. The Component Privacy Officer or PPOC reviews the PTA and forwards it to the DHS Privacy Office, who determines whether a PIA and/or SORN are required. PTA artifacts expire after three (3) years. DHS MD 047-01 defines the PTA requirements.

PTA responsibilities are provided in the following table.

Privacy Threshold Analyses Responsibilities
DHS Chief Privacy Officer
Reviews and approves the PTA
Determines whether a system is a Privacy Sensitive System
Determines whether a PIA and/or SORN are required
Uploads validated PTAs to IACS
System Owner
Submits the PTA to the Component Privacy Officer or PPOC and provide any additional information required by the DHS Chief Privacy Officer to assist in the PTA process
Component Privacy Officer or PPOC
Reviews and submits the PTA for approval and provide any additional information required by the DHS Chief Privacy Officer to assist in the PTA process.

3.14.3 Privacy Impact Assessments

A PIA is a publicly released assessment of the privacy impact of an information system and includes an analysis of the PII that is collected, stored, and shared. PIAs are required (as determined by the PTA) whenever a new information system is being developed or an existing system is significantly modified. PIAs are the responsibility of the System Owner and the Program Manager as part of the SELC process. OMB Memorandum M-03-22, DHS MD 047-01, and the *Official DHS Privacy Impact Assessment Guidance* discuss the requirements for conducting PIAs at DHS.

PIAs are one tool that DHS uses to convey public notice of information practices and the privacy impact of Department programs and activities. The Department also uses web privacy policies,

System of Records Notices, and Privacy Act Statements to provide effective public notice of program privacy practices. PIAs also document how DHS makes individuals active participants in the decision-making process regarding the collection and use of their PII.

PIA responsibilities are provided in the following table.

Privacy Impact Assessment Responsibilities
DHS Chief Privacy Officer
Reviews information systems for privacy concerns. Identifies mitigation strategies for privacy risks and document risks and mitigations in the approved PIA
Approves all PIAs
Uploads validated PIAs to IACS
System Owner
Drafts accurate and complete PIA using the DHS approved template
Identifies, as part of the PIA, privacy risks and mitigation strategies
Submits the draft PIA to the Component Privacy Officer or PPOC for review and comment
Component Privacy Officer or PPOC
Reviews draft PIAs for possible privacy risks and mitigation strategies and works with System Owners to address any privacy considerations associated with the system
Submits the complete and accurate PIA for DHS Chief Privacy Officer review and approval
Includes element counsel in review of PIAs to ensure legal compliance

3.14.4 System of Record Notices

The Privacy Act of 1974 requires a SORN when PII is maintained by a Federal agency in a system of records and the PII is retrieved by a personal identifier. A system of records is "*a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual*"[3]. The SORN describes the categories of records and individuals in the system of record; the routine uses of the data; how individuals can gain access to records pertaining to them and correct errors. The term "system of records" is not synonymous with "information system" and can include paper as well as electronic records. SORNs can be written to cover the records in a single group of records or a single information system or they can be written to cover multiple groups of records or multiple information systems.

Information systems that are considered a system of record may not be designated operational until a SORN has been published in the *Federal Register* for thirty days. OMB has issued the benchmark references for development of SORNs: *Privacy Act Implementation, Guidelines and Responsibilities*, July 9, 1975; and Appendix I, "Federal Agency Responsibilities for Maintaining

[3] *5 U.S.C. §552a(a)(5) Italics added.*

Records About Individuals" to Circular A-130. DHS has published MD 047-01, "Privacy Policy and Compliance," July 7, 2011; and *Official DHS Guidance on System of Records and System of Records Notices.* Information systems that are considered a System of Records must keep an accurate accounting of disclosures of information shared outside of the system.

OMB requires each SORN to be reviewed every two (2) years to ensure that it accurately describes the system of records. This process is called the Biennial SORN Review Process. The DHS Privacy Office works with Components to ensure that SORN reviews are conducted every two (2) years following publication in the Federal Register.

3.14.5 Protecting Privacy Sensitive Systems

OMB M-06-16, *Protection of Sensitive Agency Information* requires that agencies protect PII that is physically removed from Department locations or is accessed remotely. Physical removal includes both removable media and media in mobile devices (e.g., laptop hard drives). Please 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*:
- This Handbook's Attachment S, "Compliance Framework for Privacy Sensitive Systems"
- This Handbook's Attachment S1: "Managing Computer-Readable Extracts Containing Sensitive PII."

In addition, see Section 5.3 for PII auditing requirements and Section 5.4.1 for remote access requirements.

3.14.6 Privacy Incident Reporting

The DHS Privacy Office is responsible for implementing the Department's privacy incident response program based on requirements outlined OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007. Through close collaboration, the DHS Chief Privacy Officer, the DHS CIO, the DHS CISO, the DHS SOC, and Components must ensure that all DHS privacy and computer security incidents are identified, reported, and appropriately responded to, in order to mitigate harm to DHS-maintained assets, information, and personnel. Incidents involving (or that may involve) PII are subject to strict reporting standards and timelines.

Incident reporting responsibilities are provided in the following table.

Privacy Incident Reporting Responsibilities
DHS Personnel
Complete annual Privacy Awareness Training and Education.
Recognize Privacy Incidents.
Inform the PM of the detection or discovery of suspected or confirmed incidents involving PII; or if PM is unavailable, contact the Help Desk for the Component.
Component Privacy Officer/PPOC

Privacy Incident Reporting Responsibilities
Ensures compliance with federal laws and Departmental policy concerning safeguarding PII in consultation with the DHS Chief Privacy Officer and the Component CIO
Implements privacy incident handling process and procedures for the Component
Oversees privacy incident handling at the Component at the direction of the Chief Privacy Officer
Assesses the likely risk of harm posed by the privacy incident to determine who should handle the investigation, notification, and mitigation of the privacy incident
Collaborates with the Component IT Security Entity and the program manager to ensure a complete and accurate privacy incident report
Notifies other Component Privacy Officers/PPOCs immediately upon discovery of a privacy incident that involves the compromise of the other Component's information
Consults with Component CIO concerning privacy incident handling
Program Manager
Ensures compliance with federal laws and Departmental privacy policy concerning the operation and maintenance of information systems and programs.
Recognizes Privacy Incidents.
Understands the Component's Privacy Incident reporting process and procedures
Receives initial reports from DHS personnel regarding the detection of possible Privacy Incidents.
Consults with the Component Privacy Officer/PPOC or Component ISSM to obtain guidance concerning Privacy Incident handling and other privacy issues affecting information systems.
Determines whether a suspected or confirmed incident involving PII may have occurred.
Provides a brief preliminary written report to the Component IT security entity (e.g., ISSM or Component SOC, or Component CSIRC); or if the Component IT security entity is not available, contact the DHS SOC directly.
Assists the Component Privacy Officer/PPOC and the Component IT Security Entity with the development of facts for the Privacy Incident Report.
Provides advice, expertise, and assistance to the Privacy Incident Response Team (PIRT) as needed.
Assists with the investigation and mitigation of a Privacy Incident.
Component CISO/ISSM/Component SOC
Consults with the Component Privacy Officer/PPOC and the PM in preparing the Privacy Incident Report in SOC Online Incident Handling System
DHS SOC
Serves as the central repository and coordination point for privacy incidents Notifies Chief Privacy Officer, DHS Deputy Secretary, DHS CPO, DHS CIO, DHS Deputy CIO, DHS OGC-GLD CISO, CIO and Dep. CIO Processes and Transmits Privacy Incident Report to US-CERT Assist DHS senior officials, Component Privacy Officer/PPOCs, and the Component IT Security Entity as needed to facilitate privacy incident reporting, investigation, mitigation, and incident closure.

3.14.7 E-Authentication

Identity verification or authentication (e-authentication) is needed to ensure that online Government services are secure and that individual privacy is protected. Each DHS system must be evaluated to determine whether e-authentication requirements apply. Only federated identity providers approved through the Federal CIO Council's Identity, Credentialing, and Access Management's (ICAM) Trust Framework Provider Adoption Process (TFPAP) should be used. Components should see www.IDmanagement.gov for details regarding the Federal Identity, Credentialing, and Access Management (FICAM) initiative.

E-authentication guidance is provided in the following:

- OMB M-0404, "E-Authentication Guidance for Federal Agencies"
- NIST SP 800-63, "Electronic Authentication Guideline"

3.14.8 Use Limitation and External Information Sharing

Programs may use PII either as specified in public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Any PII shared outside the Department must be for a purpose compatible with the purpose for which the PII was collected.

DHS uses PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act or in other public notices. The DHS Chief Privacy Officer and, where appropriate, legal counsel review and approve any proposed external sharing of PII, including with other public, international, or private sector entities, for consistency with uses described in the existing privacy compliance documentation such as PIAs and SORNs or other public notice(s). When a proposed new instance of external sharing of PII is not currently authorized by the Privacy Act or specified in a notice, the Chief Privacy Officer evaluates whether the proposed external sharing is compatible with the purpose(s) specified in the notice. If the proposed sharing is compatible, program owners review, update, and republish their PIAs, SORNs, website privacy policies, and other public notices, if any, to include specific descriptions of the new uses(s) and obtain consent where appropriate and feasible. Information-sharing agreements also include security protections consistent with the sensitivity of the information being shared.

DHS programs that engage in Computer Matching Agreements (CMA) must follow established DHS guidance for ensuring that controls are in place to maintain both the quality and integrity of data shared under CMAs. See DHS MD 262-01 *Computer Matching Agreement and The Data Integrity Board*.

3.15 DHS CFO Designated Systems

DHS 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. This section provides additional requirements for these systems based on Appendix A to OMB Circular A-123, "Management's Responsibility for Internal Control." The requirements contained in OMB Circular A-123 have been mapped to the NIST SP 800-53 controls and documented in Attachment R to this Handbook, "Compliance Framework for CFO-Designated Financial Systems." The implementation guidance given in that attachment supplements the security requirements

established in DHS Sensitive Systems Policy Directive 4300A and CFO-developed financial system Line of Business requirements.

Note that Section 3.1.5 of* DHS Sensitive Systems Policy Directive 4300A *states: "Wherever there is a conflict between this section and other sections of this Policy Directive regarding requirements for CFO Designated Systems, this section shall take precedence."

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 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 CISOs/ISSMs must coordinate with their CFO organization to ensure that these requirements are implemented.

OMB A-123, Appendix A, "Implementation Plans," defines two types of system controls: Information Technology General Controls (ITGC) and Application Controls. This Handbook accounts for the ITGCs, which 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. Application controls as defined by OMB Circular A-123 provide controls over input, processing, and output of data associated with individual applications, and are not addressed in this Handbook.

A *key control* is defined as a control, or a set of controls that address the relevant assertions for a material activity or significant risk. Key controls must be identified in SPs and must be tested as part of every annual Security Control Assessment. System Owners may perform rolling compliance tests that test other (non-key) controls annually and controls that were not tested in previous years.

Documentation and testing artifacts for CFO-Designated Systems are required to be tracked and captured through the DHS Information Assurance (IA) compliance systems. These artifacts must be delivered within specified timeframes as shown in Table 1 below. Failure to do so will result in suspension of systems ATOs.

Artifact	Required Action	Frequency	Completion Deadline	Reporting Requirements
Risk Assessment (RA)	A complete RA is conducted	Annual	As determined by the Component CISO/ISSM	Report no later than (NLT) Sep 30 of each year
Security Plan (SP)	The SP is evaluated and updated	Annual	During first quarter of each FY	Report NLT Sep 30 of each year
Key Security Controls	Key security	Annual	During first	Report completion

Artifact	Required Action	Frequency	Completion Deadline	Reporting Requirements
Security Assessment Results	controls are evaluated and updated		quarter of each FY	NLT Dec 31 of each year
Disaster Recovery (DR) Plan Results	The DR plan is exercised	Annual	First quarter of each FY	Report completion NLT Dec 31 of each year
Vulnerability Assessment (VA)	A complete VA is conducted	Semi-Annual	One assessment completed during the first quarter of each FY; Second assessment completed during the third quarter.	Report completion of one assessment NLT Dec 31; report completion of second assessment NLT Jun 30
Critical Patch Installation	Installation of critical patches is verified	Semi-Annual	As determined by the Component CISO/ISSM	Report NLT Sep 30 of each year

Table 1 – Documentation and Testing Artifacts

3.16 Social Media

Social Media hosts are public content sharing websites that allow individual users to upload, view, and share content such as video clips, press releases, opinions, and other information. The DHS Office of Public Affairs (OPA) has published Terms of Service (TOS) and guidelines for posting to these sites. In some cases the Department will develop its own TOS, and in other cases it will endorse those of other Federal agencies such as the General Services Administration (GSA) or Office of Personnel Management (OPM). Due to the high threat of malware, Social Media host sites have been blocked at the Trusted Internet Connection (TIC).

There are a number of security technologies that are especially important to consider when dealing with social media issues. These include:

- Trusted Internet Connections (TIC)
- Host Configuration and Hardening
- Security Operations Center (SOC) and Network Operations Center (NOC)
- Two-Factor Authentication
- Domain Name System Security Extensions (DNSSEC) Capabilities
- Trust Zones

- Signed Code
- Patching and Anti-Virus

3.17 Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[4] addresses the privacy of individuals' health information by establishing a Federal privacy standard for health information and how it can be used and disclosed.

HIPAA prohibits the use or disclosure without the authorization of the individual or as part of an exception contained in HIPAA of Protected Health Information (PHI), electronic or otherwise, for any purpose other than treatment, payment, or health care operations for that individual.

Because of the diverse mission of DHS, it may be necessary for some Components to collect PHI as part of a larger mission requirement (for example detainee processing, disaster relief, etc.). This section applies to all Components and personnel who collect, process, or store PHI (refer to NIST SP 800-66 for further information).

3.18 Cloud Services

Cloud computing technologies allow DHS to address demand for better, faster information services and to save resources, consolidate systems, and improve security. The essential characteristics of cloud computing – on-demand provisioning, resource pooling, elasticity, network access, and measured services – provide the potential for DHS to reduce procurement and operating costs and increase the efficiency and effectiveness of services.

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program which provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that will save cost, time, and staff required to conduct redundant agency security assessments. A memorandum issued by the Federal Chief Information Officer to all agency CIOs on December 8, 2011 established FedRAMP. The goal of this Security Authorization of Information Systems in Cloud Computing Environments (FedRAMP Policy Memo) was to provide a cost-effective, risk-based approach for the adoption and use of cloud services.

The purpose of FedRAMP is to:

- Improve the consistency and quality of information security in the cloud
- Ensure trustworthy and re-usable documentation and assessment of security controls
- Provide ongoing assurance and risk assessment of select cloud services
- Enable rapid and cost-effective procurement of information systems/services for Federal agencies

4 *Public Law 104-191*

DHS is a key participant in FedRAMP. Other major participants are:

- **Federal Agency Customers**, who have a requirement for cloud technology that will be deployed into their security environment; the D/A is responsible for ensuring FISMA compliance
- **Cloud Service Providers**, who offer the willingness and capability to fulfill the cloud technology requirements of Federal Agency Customers, including security requirements
- **The Joint Authorization Board (JAB)**, comprised of CIOs from DHS, DoD, and GSA, and supported by Technical Representatives (TR) from their CISOs; the JAB reviews the security package submitted by the CSP, performs risk assessment, and grants a Provisional Authorization (P-ATO). D/As such as DHS can then use the Provisional ATO in performing their own risk assessments based on their specific security requirements avoiding duplicative assessments in reaching their ATO decision
- **Third Party Assessors** who validate and attest to the quality and compliance of the CSP provided security package
- **The FedRAMP Program Management Office (PMO)**, which provides ISSOs and manages the assessment, authorization, and continuous monitoring process for JAB reviewed services; maintains a secure repository of security packages authorized by the JAB and by Agencies; is responsible for accreditation of 3PAOs; and provides templates and guidance to support Agencies adoption of cloud computing, including sample language for use in contracts and service-level agreements
- **NIST**, who provides technical assistance to the 3PAO process, maintains FISMA standards, and establishes technical standards

DHS provides leadership to FedRAMP in Cyber security and operations, monitoring and reporting on security incidents and providing data feeds for continuous monitoring.

In addition to JAB Membership, DHS provides a team of JAB Technical Representatives who provide subject matter expertise to the DHS JAB member and recommend authorization decisions as appropriate. DHS also holds the FedRAMP role for leading Cyber Security Operations and Incident Response. This includes defining adequate, risk-based, cost-effective cyber security; the coordination of cyber security and operations; the development of continuous monitoring standards for on-going cyber security of Federal Information Systems; and develops guidance on agency implementation of the Trusted Internet Connection (TIC) program with cloud services.

Only when applying to FedRAMP for JAB review, CSPs must use a FedRAMP accredited Third Party Assessor (3PAO) to independently validate and verify the security of the cloud service. To become a FedRAMP accredited 3PAO, candidate organizations undergo a rigorous evaluation of their information assurance competencies, experience with FISMA, and experience with testing security controls. 3PAO applicants must also demonstrate technical competence in the security assessment of cloud-based information systems and meet the requirements of ISO/IEC 17020:1998 for independent organizations performing inspections. If a 3PAO does not meet FedRAMP requirements or submits sub-standard work products, they can lose their accreditation.

NIST SP 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” All uses of cloud computing by DHS will follow DHS security authorization processes and procedures to include a completed security authorization package and an ATO signed by the appropriate Authorizing Official. Those cloud systems and services which are not exempt from FedRAMP requirements will use the FedRAMP process as required by OMB. Organizations should also review Section 3.14 for applicability in cloud environments if they are dealing with privacy data.

4.0 OPERATIONAL CONTROLS

4.1 Personnel

Department of Homeland Security (DHS) systems face threats from a myriad of sources. The intentional and unintentional actions of system users can potentially harm or disrupt DHS systems and facilities and could result in destruction or modification of the data being processed, denial of service, and unauthorized disclosure of data. It is thus highly important that stringent safeguards be in place to reduce the risk associated with these types of threats.

4.1.1 Personnel Screening and Position Categorization

Personnel accessing DHS 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 system (e.g., disclosure of sensitive information, interruption of critical processing, computer fraud).

Another prudent safeguard is to ensure that individuals who support DHS systems are highly qualified technically and are adequately trained for the position they occupy. This reduces the risk of unintentional actions. While unintentional acts and accidents cannot be eliminated, effective training can help to mitigate the possibility or frequency of such 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 each contractor position are required to be determined.

Responsibilities related to personnel issues are provided in the following table.

Position Categorization and Personnel Screening Responsibilities
Component Head Requests exceptions to the DHS requirement for U.S. citizenship for non-U.S. citizens who require access to DHS systems processing sensitive information
System Owners Designate the position sensitivity level for all in-house or contractor positions that use, develop, or operate information systems
Security Managers Ensure all personnel who use, develop, or operate DHS information systems have a favorably adjudicated background investigation commensurate with the defined sensitivity level associated with their position

4.1.1.1 Background Investigations for Government Employees

DHS employees undergo the appropriate security investigations to obtain the required clearances. The following is a summary, from least to most comprehensive, of the types of security investigations as given in DHS Instruction 121-01-007, *Personnel Suitability and Security Program*:

National Agency Check (NAC) and Inquiries and Credit (NACIC): Consists of a NAC, employment/self-employment/unemployment coverage (five-year inquiry), education (five-year highest degree inquiry), residence (three-year inquiry), reference contacts (inquiry), law enforcement checks (five-year inquiry), and credit check.

NAC with Law and Credit (NACLC): Consists of a NAC, law enforcement checks (five year—inquiry or record), and credit search of national credit bureaus (seven years). This investigation will be used in conducting initial investigations for some contractor employees and for reinvestigating Federal and contract employees who need a security clearance at the CONFIDENTIAL or SECRET level.

Access National Agency Check and Inquiry: Consists of an NAC, employment/self-employment/unemployment coverage (five-year inquiry), education (five-year highest degree, inquiry), residence (three-year inquiry), reference contacts inquiry, law enforcement checks and/or record (five-year inquiry).

Limited Background Investigation (LBI): Consists of a NACIC; personal subject interview; and personal interviews by an investigator of subject's background during the most recent three (3) years.

Minimum Background Investigation (MBI): Consists of an NAC, personal interview with the individual, employment/self-employment/unemployment coverage (five-year inquiry), education (five-year highest degree, inquiry), residence (three-year inquiry), reference contacts (inquiry), law enforcement checks (five-year inquiry), and credit check (seven-year inquiry). Other than the personal interview, there are no source interviews conducted during this investigation. An MBI is the DHS minimum standard of investigation.

BI: Consists of an NAC, personal interviews with the individual and other sources, credit checks, law enforcement agency checks, residences, and employment, covering the most recent five (5) years of the individual's life or since his or her 18th birthday, whichever is shorter, provided that at least two (2) years are covered. No investigation shall be conducted prior to an individual's 16th birthday.

Single Scope Background Investigation (SSBI): Consists of an NAC; a spouse or cohabitant NAC; personal subject interview; and citizenship, education, employment, residence, law enforcement, and record searches covering the most recent ten years of the individual's life, or since his or her 18th birthday, whichever is shorter. No investigation shall be conducted for the period prior to the individual's 16th birthday.

SSBI-Periodic Reinvestigation: Consists of an NAC, personal subject interview, employment check (five years), education check (five years), residence check (current and/or most recent six-month duration), reference check, law enforcement checks (five years), former spouse (five years or since date of last investigation), and Financial Crimes Enforcement Network check.

4.1.1.2 Background Investigations for Contractor Personnel

The level of background investigation required for contractor personnel is dependent on the level of risk associated with each contractor position: high, moderate, or low. The following table depicts the type of investigation required for each risk level.

RISK LEVEL	SECURITY FORMS REQUIRED	TYPE OF INVESTIGATION REQUIRED		PRELIMINARY CHECKS REQUIREDFOR EOD / WAIVER DETERMINATION	
		IT-Computer Positions	Non-IT Computer Positions	IT Positions (waiver NTE 100 days)	Non-IT Positions
HIGH	SF 85P FD 258 Credit Release Form Non-Disclosure Statement SF 85P-S*	BI	LBI	Favorable review of forms Favorable NAC Scheduling of the BI**	Favorable review of forms Favorable NAC Submission of the LBI
MODERATE		MBI	NACIC	Favorable review of forms Favorable NAC Scheduling of the MBI	Favorable review of forms Favorable NAC + credit check
LOW	SF-85P FD-258	N/A	Favorable review of forms FP and name check	N/A	

* Only weapons-carrying contract guards must complete the SF 85P-S in addition to SF 85P

** Eligible for access only to the moderate risk level

The waiver only allows the contractor employee to commence work before the required background investigation is completed; it does not substitute for the required investigation.

4.1.2 Rules of Behavior

Rules of Behavior (ROB) for access to DHS systems and information resources are a vital part of the DHS Information Security Program. ROB inform users of their responsibilities and holds them accountable for their actions while accessing and using DHS systems, and resources capable of accessing, storing, receiving, or transmitting sensitive information. The DHS ROB applies to DHS employees, contractors, and others working on behalf of DHS.

ROB must be developed for each system, and form the basis for security awareness and training. They must clearly delineate responsibilities and the expected behavior of all individuals. Rules must be in writing; must be made available to each user to read and sign before being granted access to any system; and must state the consequences of inconsistent behavior or noncompliance.

ROB for individual systems may be inherited from organizational rules or site Rules of Behavior (for example, an individual local area network (LAN) GSS Rules of Behavior may be

automatically included as part of an organization-wide GSS ROB to which all employees and staff are held accountable).

This Handbook's Attachment G, *Rules of Behavior*, provides guidance for developing system-specific ROB and guidance for developing general ROB that apply to all DHS systems and devices capable of accessing, storing, receiving, or transmitting sensitive information.

Any person who does not comply with the appropriate set(s) of ROB is subject to penalties and sanctions, including verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, criminal or civil prosecution, or termination, depending on the severity of the violation.

Rules of Behavior that are understood and followed help ensure the security of systems and the confidentiality, integrity, and availability of sensitive information.

Rules of Behavior responsibilities are provided in the following table.

Rules of Behavior Responsibilities
System Owners
Develop and enforce Rules of Behavior for systems under their authority
ISSOs
Advise System Owners concerning the establishment and implementation of Rules of Behavior DHS systems
Ensure that Rules of Behavior for GSS and MA are included or referenced in the Security Plan (SP)
Ensure users read and sign general Rules of Behavior for use of DHS systems and resources
Ensure that users read and sign specific Rules of Behavior for systems to which they will be given access
Users
Adhere to all Rules of Behavior for the systems to which they have been granted access

4.1.3 Access to Sensitive Information

To protect sensitive information and limit the damage that can result from accident, error, or unauthorized use, the principle of least privilege must be applied.

The principle of least privilege requires that users be granted the most restrictive set of privileges (or lowest clearance) needed for performance of authorized tasks. Users should be able to access only the system resources needed to fulfill their job responsibilities. Application of this principle ensures that access to sensitive information is granted only to those users with a valid need to know.

Access to sensitive information responsibilities are provided in the following table.

Access to Sensitive Information Responsibilities
System Owners
Ensure that prior to being granted access to information contained in DHS systems, users have a valid *need to know*
Ensure that prior to being granted access to sensitive information resources, users have the appropriate level of clearance
ISSOs/System Administrators
Ensure that prior to being granted access to DHS systems, users have a valid requirement
Ensure that prior to being granted access to sensitive information resources, users have the appropriate level of clearance

4.1.4 Separation of Duties

Separation of duties is intended to prevent a single individual from being able to disrupt or corrupt a critical security process.

Separation 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 subverta 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 separation of duties is the separation 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 Information Systems Security Officer (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 a Component does not have sufficient manpower resources necessary to meet strict separation 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.

Responsibilities related to separation of duties are provided in the following table.

Separation of Duties Responsibilities
System Owners
Ensure that personnel work assignments comply with DHS policy regarding separation of duties for sensitive systems
ISSOs
Ensure that controls that enforce separation of duties are in place
Ensure that compensating controls are in place for situations in which strict separation of duties cannot be fully implemented

4.1.5 Information Security Awareness, Training, and Education

A key objective of an effective Information Security Program is to ensure that each employee understands his or her role and responsibilities and is adequately trained to perform them. DHS cannot protect the confidentiality, integrity, and availability of its systems and the information they contain without the knowledge and active participation of its employees in the implementation of sound security principles.

All users of Federal information systems are required by 5 CFR part 930, subpart C, as revised, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. Training for new system users must occur before they are allowed access to systems. OMB Circular A-130 Appendix III, "Security of Federal Automated Information Resources," requires that persons be trained in their responsibilities and in the Rules of Behavior for using GSS and major applications (MA).

Information security training is required to be addressed in the Security Plan for each system. Additionally, Component CISOs/ISSMs[5] prepare and submit an annual training plan for information security awareness, training, and education to the DHS Information Systems Security Training Program Director. Plans are required to follow the guidance in the DHS Information Technology Security Awareness, Training and Education Plan template, issued by the DHS Information Systems Security Training Office.

OPM requires Federal agencies to provide training to the following groups within 60 days of their appointment:[6]

- Executives
- Program and functional managers
- Information resources management
- Security audit personnel

5 *CISO: Chief Information Security Office; ISSM; Information Systems Security Manager*

6 In 5 CFR Part 930,

- Information system managers and operations personnel

National Institute of Standards and Technology (NIST) SP 800-16, "Information Technology Security Training Requirements: A Role and Performance-Based Model," provides detailed guidelines for developing a robust training program.

4.1.5.1 Initial Awareness

New employees are required to complete an initial information security awareness course and sign appropriate Rules of Behavior as part of their orientation process. Also, Components are required to provide an initial awareness course to newly hired contractor staff or ensure that the contractors provide an equivalent course.

Completion of the appropriate awareness course is mandatory before access is granted to any DHS system or information resources. Records of the training must be maintained to verify compliance. Records must include name and position, the type of training received, and the date and cost of training.

Appropriate media for providing this initial awareness include seminars, presentations, awareness videos, and computer-based training.

4.1.5.2 Refresher Awareness

Components must provide an annual information security awareness refresher course to all users or ensure that contractors provide an equivalent refresher course for their staff. Completion of the refresher course is mandatory. Unless the respective Component CISO issues a waiver, user accounts and access privileges, including access to email, will be disabled for those who have not received annual refresher training. Records of training must be maintained to verify compliance. Records must include name, position, the type of training received, and the date and cost of training.

Appropriate media for providing this initial awareness include seminars, presentations, awareness videos, and computer-based training.

Additional awareness sessions must be conducted whenever there is a significant change in the information security environment or procedures or when an employee enters a new position involving the handling of sensitive information.

4.1.5.3 Ongoing Awareness Activities

Components must reinforce the awareness message throughout the year through the use of posters, newsletters, email messages, trinkets with a security message, and other appropriate communication media.

4.1.5.4 Role-Based Training

DHS personnel, contractors, and others working on behalf of DHS that have significant security responsibilities (e.g., ISSOs, network administrators, system administrators, AOs) must receive annual specialized training specific to their security responsibilities. Specialized security-related training must also be provided to senior managers, System Owners, and Project Managers.

The level of training is required to be commensurate with the individual's duties and responsibilities. Components must track, by name and position, the type of the training received, and the dates and cost of the training.

Information security awareness, training, and education responsibilities are provided in the following table.

Information Security Awareness, Training, and Education Responsibilities
Component CISOs/ISSMs
Establish overall policy for information security awareness, training, and education
Provide guidance on preparing and attending security awareness and training sessions
Submit a training plan outlining plans for Information Security Awareness, Training, and Education for the year to the DHS Information Security Training Program Director
Analyze security awareness and training statistics submitted by the ISSOs and CORs and submit a summary of these statistics to the DHS Information Security Training Program Director on a quarterly basis
ISSOs
Ensure that all new employees, including contractors, complete an initial security awareness course as part of their orientation
Unless a Component CISO/ISSM waiver is issued, disable all accounts and access privileges, including access to email, of those DHS users who failed to complete the annual security refresher course
Ensure that all users read and sign the appropriate Rules of Behavior prior to being granted access to systems and applications
Implement annual awareness refresher training for employees and support contractors involved in the management, use, or operation of DHS systems
Maintain a record of security awareness and training that includes the name and position of the person trained, the type of training, the date of the training, and the cost of the training
Submit statistics on initial and refresher security awareness and training to the Component CISO/ISSM, on a quarterly basis
Implement additional training for personnel when there is a significant change in the system security environment or in procedures, or when an employee enters a new position involving the handling of sensitive information
CORs
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

Information Security Awareness, Training, and Education Responsibilities
Ensure that contractor security awareness and training statistics are provided to the Component CISO/ISSM on a quarterly basis

4.1.6 Separation from Duty

This section addresses the procedures to be followed when an employee, contractor, or other individual working on behalf of DHS terminates employment or transfers to another organization.

In most circumstances, an individual's departure is amicable; allowing him or her to complete his or her duties and obligations through the last day. When the employee or contractor demonstrates resentment, the site security office should assist in creating a prudent plan of action.

In all cases, Components are required to adhere to the following:

- Revoke all authorizations
- Retrieve hard and soft copy sensitive information
- Retrieve all keys, badges, and other access devices
- Change locks
- Retrieve Government-owned equipment including but not limited to laptops, cell phones, portable electronic devices (PED), secure ID tokens.
- Conduct exit interview

Responsibilities related to separation from duty are provided in the following table.

Separation from Duty Responsibilities
System Owners/Senior Site Managers Implement procedures to ensure appropriate system access privileges are revoked for employees or contractors who either leave the Component or are reassigned to other duties
Supervisors Notify system administrators in writing when employees or contractors no longer require access to DHS systems Retrieve all sensitive data from departing employees and contractors
Network/System Administrators Disable or delete user accounts when notified that an individual's access to DHS systems is reassigned or terminated
Site Security Officers Change combinations to all locks and safes whenever an employee or contractor with access has been reassigned or terminated

Separation from Duty Responsibilities
Collect all keys, badges, and other devices used to gain access to premises, information, or equipment from employees and contractors who have been terminated or reassigned
Employees, Contractors, or Others Working on Behalf of DHS
Turn in laptops, cell phones, mobile devices, secure ID tokens, and other Government-owned devices to the local property administrator in accordance with local procedures when reassigned or terminated

4.2 Physical Security

Information systems must be physically and environmentally protected to prevent unauthorized disclosure, denial of service, destruction, or modification. Physical security represents the first line of defense against intruders attempting to gain physical access to systems and must be addressed during each step of the risk management cycle. Cost-effective controls are documented in the Security Plan and are evaluated during the Security Control Assessment. Residual risks are documented in the Security Authorization Process package and reviewed annually.

4.2.1 General Physical Access

General physical access controls restrict the entry and exit of personnel from an area, such as an office building, data center, or room where sensitive information is accessed, stored or processed. Such controls protect against threats associated with the physical environment. Components should review the effectiveness of general physical access controls during business hours and at other times. Control effectiveness depends on the characteristics of the controls, their implementation, and their operation.

General physical access responsibilities are provided in the following table. Specific requirements are given in DHS Sensitive Systems Policy Directive 4300A, Section 4.2.1.

General Physical Access Responsibilities
Facility Managers
Ensure that physical controls are in place
Ensure that environmental controls are in place
Ensure that physical and environmental controls are in working order at all times
Ensure that access control logs are maintained and reviewed for the facility and all computer rooms
Site Security Officers/ISSOs
Provide specific security briefings to DHS employees and contractors
Assess the adequacy of physical security controls as part of the risk management cycle
Change combinations to locks on security containers housing sensitive information, funds, and other valuables that must be safeguarded
Conduct periodic inspections of offices and areas under their jurisdiction, during or after working

General Physical Access Responsibilities
hours, to ensure that sensitive and proprietary materials are being adequately safeguarded
Ensure that security violations are appropriately reported and investigated, in accordance with DHS requirements
Provide oversight of the issuing and return of service badges, credentials, and identification documents, and ensure proper reporting of their loss or theft
Apply security disciplines to the contractor environment
Ensure that Government-owned and controlled property, funds, and valuables are properly safeguarded and accounted for
Ensure the physical security of information systems within their jurisdiction
Ensure that physical and environmental security controls are addressed in the Security Plan
Address physical security as an integral part of the risk management process
Ensure that physical security risks are reviewed and evaluated throughout the Systems Engineering Life Cycle (SELC)
Users
Adhere to established security policies
Display building passes or other ID when required
Challenge individuals who are not in compliance with established requirements
Ensure that uncleared visitors are escorted at all times

4.2.1.1 Physical Controls

Physical controls include barriers, badges, guard or security forces, supporting infrastructure, contingency and emergency support, lighting, facility intrusion detection systems, and surveillance systems. Standards for physical security must be based on an analysis of mission criticality, severity of impact levels, local criminal and intelligence threats, and the value of the equipment and data contained within the facility being protected.

Security personnel must ensure that physical security controls are considered throughout a system's life cycle and reviewed in conjunction with the annual self-assessments. The following controls should be considered and included in the appropriate Security Plan:

- Controlled access to building (e.g., physical building access, guards)
- Controlled access to computer room(s)
- Locks
- Key control procedures
- Keypads and cipher locks
- ID badges (worn above the waist area)
- Visitor logs

- Biometric devices
- Access control logs (to the building)
- Access control logs (to the computer rooms and facility)
- Motion detectors
- Intrusion detection devices
- Property passes
- Additional controls

Not all of these features will be necessary for every facility. ISSOs and site security officers must determine which security features are warranted.

4.2.1.2 Building Passes

Building passes must be issued and displayed by all individuals at all facilities that store or process sensitive information. Passes should be displayed above the waist and below the neck with the photo side facing out. Each visitor must be issued a temporary building pass which must be turned in upon leaving the facility.

Persons not displaying proper credentials should be challenged. If there is any doubt as to their authorization, they should be escorted from the area and local security personnel should be notified.

Security personnel and supervisors at all management levels must ensure that all staff, contractors, and others working on behalf of DHS are aware of this requirement and periodically reinforce it during staff meetings through email, and by other means. Where practical, challenge procedures should be posted.

4.2.1.3 Property Removal

Removal of items from DHS facilities must be controlled and documented.

4.2.1.4 Loss or Theft of Property

Any missing property, whether lost or stolen, must be reported.

4.2.1.5 Environmental Controls

In addition to the physical security controls discussed above, facility managers and security administrators must also ensure that environmental controls are established, documented, and implemented to provide needed protection in the following areas:

- Fire protection, detection, and suppression
- Water damage risk reduction, detection, and corrective measures, and devices for water hazard prevention
- Electronic power supply protection, to include uninterruptible power supplies for multi-use systems and surge protectors for stand-alone systems
- Temperature and humidity recording, monitoring, and alert systems
- Housekeeping protection from dirt and dust

- Combustible cleaning supplies protection (not to be kept in computer areas)
- Appropriate personnel safety features (evacuation routes specified)
- Emergency exit provisions, such as equipping emergency and exit-only doors with hardware that permits immediate egress in the event of an emergency

4.2.1.6 Fire Protection

Fire protection systems should be serviced by professionals on a recurring basis to ensure that the systems stay in proper working order. The following should be considered when developing a fire protection strategy:

- When a centralized fire suppression system is not available, fire extinguishers should be readily available:
  - Facilities should make available/provide Class C fire extinguishers (which are designed for use with electrical fire and other types of fire).
  - Fire extinguishers should be located in such a way that a user would not need to travel more than 50 feet to retrieve one.
- Fire drills must be conducted annually to ensure that all personnel are familiar with their responsibilities.

4.2.1.7 Electronic Power Supply Protection

Electrical power must be filtered through an uninterruptible power supply (UPS) system for all servers and critical workstations and surge suppressing power strips used to protect all other computer equipment from power surges.

4.2.1.8 Temperature and Humidity Control

The following should be considered when developing a strategy for temperature and humidity control:

- Temperatures in computer storage areas should be held between 60 and 70 degrees Fahrenheit. Most systems will continue to function when temperatures go beyond this range, but the associated risk to data is increased. (Check individual system documentation for the proper levels.)
- Humidity should be at a level between 35 percent and 65 percent. Most systems will continue to function when humidity goes beyond this range, but the associated risk to data is increased. (Check individual system documentation for the proper levels.)
- Low humidity can result in static, and high temperature can damage sensitive elements of computer systems. (Check individual system documentation for the proper levels.)

Security personnel should obtain a device that will sound an alarm and send out an automatic notification (via email or pager) when the operating environment exceeds recommended boundaries.

4.2.1.9 Housekeeping Considerations

Housekeeping is another important area to monitor.

- Subfloors (where installed) should be cleaned annually.

- If the computer room has carpet it should be of the antistatic variety. This also applies to areas that house workstations.
- Dusting of hardware and vacuuming of work areas should be performed weekly with trash removal performed daily. Dust accumulation inside of monitors and computers is a hazard that can damage computer hardware.
- Cleaning supplies should not be stored inside the computer room.

4.2.1.10 Personnel Safety Features

The facility manager should brief all personnel on emergency procedures including:

- Evacuation procedures
- Location of emergency exits
- Location of emergency equipment such as fire extinguishers and first-aid kits

4.2.1.11 Emergency Exits

Emergency exits should be clearly marked and all personnel should be familiar with established evacuation routes.

4.2.2 Sensitive Facility

Additional environmental and physical controls, based on a risk analysis, should be considered for facilities supporting large-scale operations, such as enterprise servers and telecommunication facilities.

4.3 Media Controls

Storage media that contain sensitive information must be controlled so that the information is protected. Storage media include but are not limited to the following:

- Magnetic storage media – Including reel and cassette format magnetic tapes; magnetic disks, including hard disk drives, floppy disks and diskettes, and disk packs; magnetic cards; and magnetic memory devices, including core memory and magnetic bubble memory
- Optical storage media – Including optical cartridges, laser disks, compact disks (CD), digital video disks (DVD), Magneto-Optical (MO) disks, holographic devices, and optical tapes
- Solid-state storage media – Including Random Access Memory (RAM), Read Only Memory (ROM), Field Programmable Gate Array (FPGA) devices, Personal Computer Memory Card International Association (PCMCIA) cards, Flash cards, Smart Cards, and Universal Serial Bus (USB) drives (also called flash drives, jump drives, and thumb drives)
- Hard-copy storage media – Including paper and microforms (e.g., microfilm and microfiche)

4.3.1 Media Protection

Additional security risks are 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. Proper storage enhances protection against unauthorized disclosure.

All media containing sensitive information must be labeled and kept in a secure location. Backup and archive media must be sent to an off-site location as identified in the appropriate business continuity and contingency plans.

Media protection responsibilities are provided in the following table.

Media Protection Responsibilities
DHS CISO
Establishes and enforces DHS policy relating to labeling, storage, media reuse, and disposal of DHS equipment
System Owners
Ensure that any special storage requirements are communicated to the Project Manager and system administrators
System/Network Administrators
Ensure that sensitive information is stored in a locked container or in an area with adequate access controls to prevent unauthorized access, disclosure, damage, modification, or destruction
Ensure that recipients of sensitive information have a valid "need to know" and proper authorization
Ensure that copies of backups are stored at secure offsite locations
Facility Managers
Ensure that sensitive information is stored in a locked container or in an area with adequate access controls so as to prevent unauthorized access, disclosure, damage, modification, or destruction
Establish both onsite and offsite storage locations
Establish and maintain an inventory accounting system for all media entering or leaving a media storage area.
Ensure that inventory is verified at least semiannually
Ensure that backup storage facilities meet the minimum requirements enumerated in Section 4.11, Information and Data Backup
ISSOs
Ensure that media are stored in accordance with the requirements enumerated in this handbook
Ensure that storage requirements are addressed in the Security Plan and Rules of Behavior

4.3.2 Media Marking and Transport

DHS processes, stores, and transmits many types of sensitive information. Appropriately labeling the media helps ensure that all recipients of the material are aware that the information requires protection.

Note: If information with different levels of sensitivity is combined, the total package must carry the sensitivity level of the information that has the greatest sensitivity.

The following definitions apply within this section:

- **Hardcopy Material** – Printed material, including reports, emails, briefings, manuals, guidance, letters, and memoranda
- **Label** – A piece of information that indicates the sensitivity level of an object and the information it contains. A label may be internal or external as follows:

– **Internal Label** – A marking that reflects the sensitivity of the information within the confines of the medium

– **External Label** – Has a visible marking on the outside of the medium, or a cover that reflects the sensitivity of the information contained

- **Storage Media** – Includes but is not limited to magnetic storage media such as hard disk drives and diskettes; optical storage media such as CDs and DVDs; solid-state storage media, including USB drives; and hardcopy materials, including reports, emails, briefings, manuals, guidance, letters, and memoranda.

Terminals, desktop and laptop computers, and other mobile computing devices not authorized to process classified information should be appropriately labeled, especially in environments where both sensitive information and classified information are processed. ”This Medium is Unclassified” labels are available through GSA (standard form 710).

Media marking responsibilities are provided in the following table.

Media Marking Responsibilities
DHS CISO Establishes and enforces policy relating to labeling, storage, reuse, and disposal of media containing sensitive information **System Owners** Ensure that mission security needs are communicated to Project Managers and system administrators **Project Managers** Implement electronic marking requirements and warning banners for automated systems **System Administrators** Implement electronic marking requirements and warning banners on their systems **ISSOs** Ensure that sensitive systems and information are appropriately identified and that sensitivity and criticality levels are established for each system Ensure that marking requirements are addressed in the SP and that areas of noncompliance are identified Ensure that automated system and site personnel understand and are adequately trained in the identification and marking of sensitive information Ensure that marking procedures and warning banners are reviewed with all personnel periodically, such

Media Marking Responsibilities
as during annual Computer Security Awareness sessions
Ensure that all users are aware of the value and sensitivity of information
Ensure that users understand their responsibilities for safeguarding sensitive DHS information and know how to fulfill their responsibilities
Ensure that procedures are in place to ensure that all personnel follow guidelines and procedures for marking media containing sensitive information

4.3.3 Media Sanitization and Disposal

Media containing sensitive information must be sanitized prior to reuse or disposition (i.e., disposal or recycling; return of leased media to the owner; return of defective or inoperable media for repair or replacement) in order to protect sensitive information from unauthorized disclosure.

Media sanitization responsibilities are provided in the following table.

Media Sanitization Responsibilities
Site Managers
Allocate resources to meet media sanitization requirements
Enforce media sanitization requirements
Component CISOs/ISSMs
Develop and implement media sanitization procedures for storage media that are to be disposed of, recycled, reused, returned to the owner, or returned for repair or replacement
ISSOs
Ensure that media sanitization requirements are addressed in the SP and Security Operating Procedures
Maintain records of the sanitization and disposition of sensitive storage media
System/Network Administrators
Ensure that storage media for disposal, recycling, or reuse are properly sanitized
Ensure that leased storage media are properly sanitized before they are returned to the owner
Ensure that defective or inoperable storage media are properly sanitized before they are returned to the vendor or manufacturer for repair or replacement
Ensure that defective or inoperable storage media that cannot be sanitized are physically destroyed and disposed of
Periodically test degaussing equipment to ensure proper operation
Users
Ensure the safekeeping of sensitive storage media
Notify ISSO or Site Security Manager when media containing sensitive information are no longer

Media Sanitization Responsibilities
required

NIST SP 800-88, *Guidelines for Media Sanitization*, provides guidelines for the sanitization of numerous types of information storage media, including:

- Magnetic disks (floppy disks; hard drives; USB removable media and drives, flash drives, and memory sticks with hard drives; etc.)
- Magnetic tapes (reel and cassette format magnetic tapes)
- Magnetic cards
- Optical disks (CDs, DVDs)
- Memory
- Hard copy (paper and microforms)
- Networking devices such as routers
- Handheld devices such as cell phones and personal digital assistants (PDA)
- Equipment (copy machines, fax machines)

This Handbook provides information on the sanitization requirements for media containing classified information.

NIST SP 800-88, "Guidelines for Media Sanitization" identifies sanitization options for various storage media. Sanitization options depend on the type of storage medium (e.g., hard drive, CD or DVD, hard copy), intended disposition of the medium (e.g., reuse, disposal), and FIPS 199 categorization for the confidentiality security objective (see Section 3.9.1, FIPS 199).

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:

- ***Clearing*** is removal of information stored on media in such a way that the information is irretrievable through means such as robust keyboard attacks or the use of data, disk, or file recovery techniques. For magnetic media such as hard drives and diskettes, simple deletion of files is not sufficient for clearing, as the deleted data can be retrieved by various recovery utilities. Overwriting the information with random data, however, will clear the media of information and will help ensure that the information is irretrievable except perhaps by advanced laboratory techniques. Overwriting cannot be used for magnetic media that are damaged or not writeable. In such cases, the media must be physically destroyed.
- ***Purging*** is removal of information stored on media in such a way that the information is irretrievable through any means, including advanced laboratory techniques. Executing the firmware Secure Erase command and degaussing are examples of acceptable methods for purging. Degaussers expose the medium to a strong magnetic field, which effectively erases the information (a degausser designed and approved for the type of medium being purged is required). Be aware that degaussing also destroys hard drives, as the firmware that manages

the drive is also purged during the degaussing process. Degaussing is effective only on magnetic media such as hard drives, diskettes, and magnetic tapes. It is not effective on optical media such as CDs and DVDs.

- ***Destruction*** of media is the ultimate form of sanitization. Physical destruction can be accomplished through disintegration, incineration, pulverizing, shredding, and melting. Destruction of media should be conducted only by trained and authorized personnel. Safety, hazmat, and special disposition needs should be identified and addressed prior to conducting any media destruction.

Sanitization also requires the removal of all labels, markings, and activity logs.

Steps for sanitizing of media are as follows:

- Determine the categorization (i.e., low, moderate, or high impact) for the confidentiality security objective
- Determine whether the media will be disposed of or reused (either within or outside of the organization)
- Use Figure 3 to determine the appropriate method of sanitization
- Refer to NIST SP 800-88, Appendix A and Table A-1, for sanitization options for the type of medium to be sanitized
- Validate and document the sanitization of the medium. NIST SP 800-88, Appendix F, provides a sample sanitization validation form
- Sensitive media can be shipped to facilities for clearing, sanitization, or disposal (The National Security Agency (NSA) may accept sensitive media for destruction. For more information and for requirements, contact NSA Classified Material Conversion Customer Service at (301) 688-6672.)

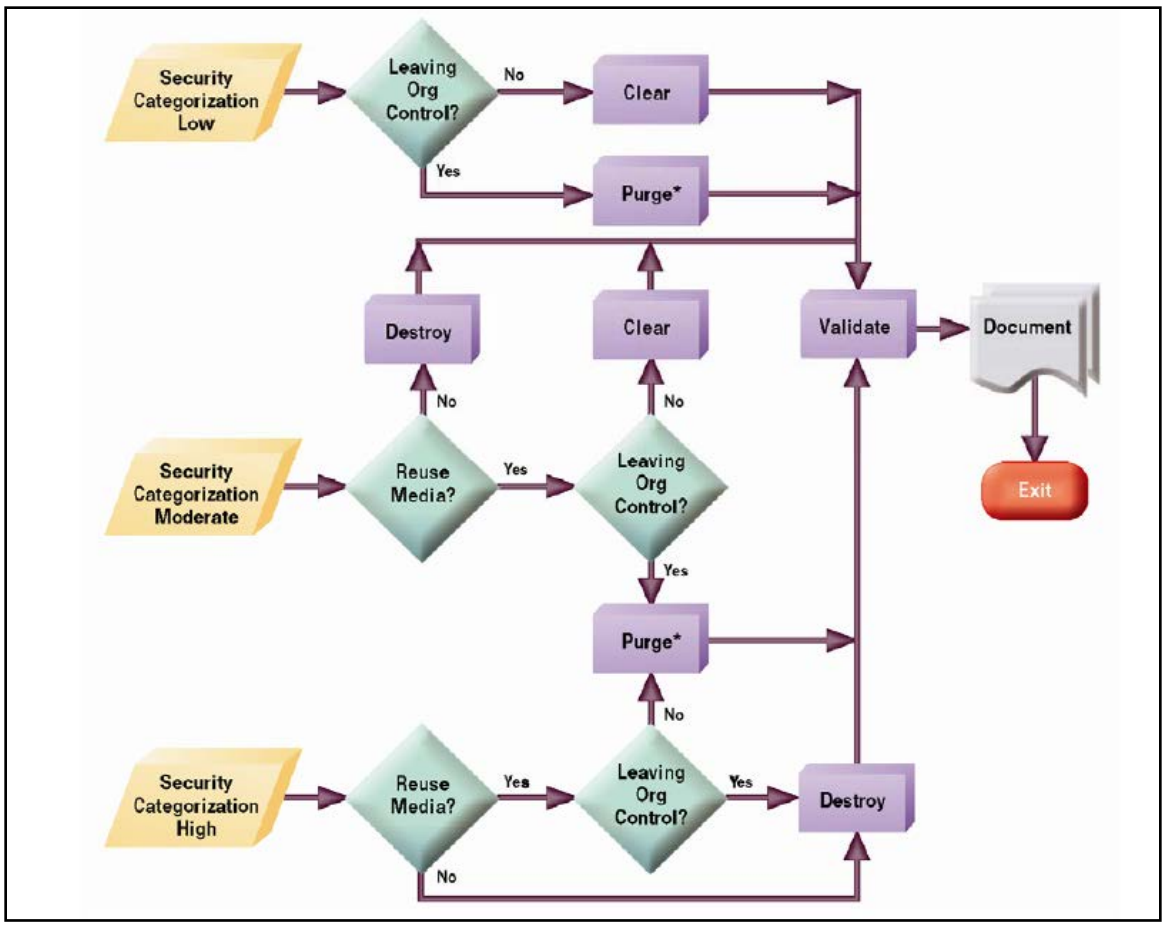


Figure 2 – Flowchart depicting the process for selecting media sanitization method, by categorization of impact for the confidentiality security objective.
(Adapted from NIST SP 800-88)

4.3.4 Production, Input/Output Controls

Sensitive information should be sent through means that limit the potential for unauthorized disclosure regardless of the method of transmission. Since information transmitted over unencrypted electronic links such as telephone lines may be intercepted, custodians of sensitive information should decide whether specific information warrants a higher level of protection, such as that afforded by a secure fax, secure phone, or other encrypted means.

Sensitive information may be sent via the U.S. Postal Service, Army Post Office (APO), commercial messenger, or **unclassified** registered pouch, provided it is packaged in a way that does not disclose its contents (e.g., double-enveloped).

In data center environments, procedures should be implemented to account for the receipt of input and output media (paper, magnetic, optical, etc.). Rosters of persons authorized to submit or receive input or output should be maintained. Logs documenting transfer of sensitive data via third party services such as mail and courier must be maintained.

Responsibilities related to production, input/output controls are provided in the following table.

Production, Input/Output Control Responsibilities
Component CISOs/ISSMs
Develop and enforce policy relating to input and output of sensitive information
Facility Managers
Ensure that sensitive information is transmitted and received in accordance with DHS policy
ISSOs
Ensure that the Security Plan addresses transmission of sensitive material
Ensure that users have authority to access only information for which they have a valid "need to know"
Ensure that sensitive information is transmitted in a secure manner

4.4 Voice Communications Security

This section addresses vulnerabilities inherent in voice communications and the operational controls needed to mitigate the associated risks. Voice communication security includes Private Branch Exchange (PBX) systems, telephone usage, and voice mail. If Components choose to encrypt their voice communications, Advanced Encryption Standard (AES) encryption per FIPS 140-2 must be used.

4.4.1 Private Branch Exchange

A PBX is a computer-based switch that acts as a small, in-house telephone exchange for the organization that operates it. Failure to secure a PBX system can result in toll fraud as well as theft of proprietary, personal, and confidential information. Moreover, an attacker could use the call tracking features of an unsecured PBX for traffic analysis to determine possible patterns of response to a planned intrusion. PBX protection is a high priority.

Potential threats to a PBX include:

- Unauthorized access
- Traffic analysis
- Theft of service
- Disclosure of information
- Data modification
- Denial of service

PBXs are sophisticated computer systems that are vulnerable to many of the same threats associated with general purpose operating systems. There are two important ways in which PBX security differs from conventional operating system security:

- **External access/control** – PBXs typically require remote maintenance by vendors. Local administrators often have the manufacturer remotely install updates, which requires remote maintenance ports and access to the switch by a potentially large pool of outside parties.

- **Feature richness –** The wide variety of features available on PBXs, particularly administrative features and conference functions, allow for the possibility of unexpected attacks. An attacker may eavesdrop by using features in a manner not intended by its designers. Features may also interact in unpredictable ways, leading to system compromise even if each element of the system conforms to its security requirements and the system operation and administration are correct.

PBX security responsibilities are provided in the following table.

PBX Security Responsibilities
Component CISOs/ISSMs
Provide guidance concerning appropriate PBX-related security training to include:
– Types of information personnel should not release to callers
– Security requirements for new PBX systems (e.g., disable test accounts, passwords, and shortcut keys) and for maintenance activities for distribution to vendors
Site Managers
Ensure that employees and others with access to the facilities have agreed to and signed a PBX policy statement
Ensure that PBX contracts and maintenance agreements include information on disputes, how they are settled, and the appeals process. Obtain approval from legal team before implementing
Explicitly include the requirements for integrity, availability, and confidentiality protection in the PBX, and directly address liability in PBX contractual agreements
Develop specific guidelines on acceptable and unacceptable use of telecommunications within the organization, and specify how the PBX policy deals with actions not explicitly covered by the general information security policy
ISSOs
Address PBX issues in annual awareness sessions for all employees
Identify, in the policy statement, the personnel or position(s) responsible for telephone usage
Ensure that agreements with the local exchange carrier (LEC), the inter-exchange carrier (IXC), and the equipment vendors allow only authorized personnel to request service level changes, and to report errors
Verify all toll calls billed against PBX traffic reports
Ensure that internal PBX audits include verification that all records are in electronic form
Ensure that internal information systems auditors complete an audit of each PBX system at least once a quarter
Ensure that all personnel with access to the PBX or connected equipment have signed employee agreements including PBX-related material
Test audit mechanisms at least quarterly
Test audit computers periodically

PBX Security Responsibilities
Ensure external auditors do blind external testing
PBX Administrators
Identify the personnel or position(s) responsible for telephone usage in the PBX policy statement
Ensure that agreements with the LEC, the IXC, and the equipment vendors allow only authorized personnel to request service level changes, and to report errors
Verify all toll calls billed against PBX traffic reports
Ensure that internal PBX audits include verification that all records are in electronic form
Ensure that internal information systems auditors complete an audit of each PBX system at least once a quarter
Ensure that all personnel with access to the PBX or connected equipment have signed employee agreements including PBX-related material
Test audit mechanisms at least quarterly
Test audit computers periodically
Ensure that external auditors perform blind external testing
Site Telephone Technical Support
Clearly marks circuit numbers on channel banks, communications service units (CSUs), data service units (DSUs), and modems
Clearly labels main distribution frames (MDF)s and intermediate distribution frames (IDF)s
Fully documents procedures for making PBX software and hardware changes, using signed checklists to record all changes as they occur
Identifies third party calls on phone bills and flag them on automated analysis
Generates and keeps full call audit records in paper and electronic forms
Follows procedures to ensure the periodic dump of all PBX parameters and automatic comparison to the previous dump; report differences to management
Follows procedures to determine the frequency of the periodic dump and comparison as a normal part of risk management
Stores PBX backups off-site; verifies the media by reading back in; and periodically tests the media on backup equipment to assure that they work properly
Ensures that a complete dump of internal parameters is reconciled with previous dumps after completion of remote maintenance
Records all transactions in an external computer system
Ensures that systems cannot redirect incoming calls from outside lines to make outside calls
Records and prints all call details
Stores records on a write once read many (WORM) disk for additional assurance

4.4.1.1 Maintenance Vulnerabilities

PBX manufacturers may include features useful on occasions when on-site maintenance personnel cannot resolve problems. For example, the manufacturer could instruct maintenance personnel to configure and connect a modem to the maintenance port, allowing remote access to certain special features in order to resolve problems without sending a representative to the PBX site. Use of such remote connections must be controlled and they must only be made available as needed in response to a particular problem. Use must also be logged, and supervised. These types of features must not be accessible via accounts held privately by the manufacturer. Proper password procedures must be enforced. It is only by exception that passwords may expire in a shorter period (e.g., thirty days) or be single use (e.g., a secure remote access device). All such access and changes to the PBX data and configuration must be logged.

Examples of these special features include:

- **Database upload/download utility** – Allows the manufacturer to download the database from a system that is malfunctioning and examine it at their location to try to determine the cause of the malfunction
- **Database examine/modify utility** – Allows the manufacturer to remotely examine and modify a system's database to repair damage caused by incorrect configuration, design bugs, or tampering
- **Software debugger/update utility** – Permits the manufacturer to remotely debug a malfunctioning system. It also allows the manufacturer to remotely update systems with bug fixes and software upgrades.

These features are subject to intrusion, and could provide dangerous access to the PBX if misused. To mitigate the associated risks, ISSOs and site managers must:

- Ensure that remote maintenance access is not operational. Whenever possible, some involvement of local personnel in opening remote maintenance ports is required.
- Install two-factor (i.e., two different mechanisms) strong authentication on remote maintenance ports. Smart Card based systems or one-time password tokens, used in addition to conventional login/password functions, make it much more difficult for attackers to breach the system's security.
- Keep maintenance terminals in a locked restricted area
- Locate the PBX equipment in a locked restricted location that does not indicate what it contains (e.g., do not post a sign saying "PBX room")
- Turn off maintenance features when not needed
- Verify that non-U.S. Citizens do not perform maintenance

4.4.1.2 Software Loading and Update Tampering

A PBX is particularly vulnerable to software tampering when software is initially loaded and whenever software updates/patches are being applied. The PBX is particularly vulnerable to software tampering. An adversary could intercept a software update sent to a PBX administrator. To mitigate the risks associated with these vulnerabilities, ISSOs and site managers must:

- Make passwords resistant to cracking by automated tools
- Understand that conventional error detection codes such as checksums or cyclic redundancy checks (CRC) are not sufficient to ensure tamper detection. Strong error detection based on cryptography provides better protection.
- Ensure that PBX boot disks, utilities, logs and records receive more protection than that for typical office software. Strong physical security should be provided, and these items must be appropriately labeled (see Sections 4.3.2 and 4.11 this Handbook).
- Shred printouts and sanitize media before discarding

4.4.1.3 User Features

The many features that make PBXs easy to configure and use have led to an expansion of vulnerabilities. These features include:

- Attendant console/override/forwarding/conferencing
- Automatic call distribution (ACD)
- Override (intrude)
- Diagnostics
- Feature interaction

To mitigate the risks associated with these vulnerabilities, ISSOs and site managers must:

- Connect the attendant console to the PBX with a different physical connection than that of the telephone instruments
- Use a line configuration feature if the attendant console connects to the PBX in the same manner as the telephone instruments. Such a feature could require specific line configuration for use with an attendant console. This would prevent the replacement of a telephone instrument with an attendant console to gain access to administrative features.
- Ensure that only essential features are activated
- Log any changes to the configuration (software, database or physical) of the device
- Activate and periodically check any logging facilities provided by the device
- Perform periodic reviews of security facilities, confirming proper configuration and proper correlation of manual logs, device logs and other records

4.4.2 Telephone Communications

Unsecured telephones are not to be used to discuss classified security information. Moreover, care must be exercised in discussing sensitive information. Adequate protection of sensitive information requires awareness of the various risks related to telephone equipment and conversations. Components are required to ensure that users are cognizant of social engineering techniques used to obtain information over the telephone, including passwords and access codes.

Telephone communications responsibilities are provided in the following table.

Telephone Communications Responsibilities
DHS CISO Establishes and enforces policy relating to telephone communications **ISSOs** Ensure that users are aware of the telephone communications policy **Users** Adhere to the telephone communications policy that requires them not to discuss classified information over the telephone and to exercise care when discussing sensitive information

The following vulnerabilities of unsecured telephone systems can result in unintentional transmission of classified or sensitive information. Commonly accepted best practices dictate that users be made aware of these vulnerabilities and exercise extreme caution when discussing sensitive information on unsecured phones. Unsecured phones are never used to discuss classified information.

- Telephones that are "on-hook" can intercept voice communications by design, by modification, or by attachment of monitoring devices.
- Cordless telephones generate signals that can be monitored.
- Speakerphones can pick up nearby conversations containing sensitive material.
- Telephone answering devices can be accessed to retrieve sensitive information.
- Call forwarding options can be used to redirect sensitive messages.
- Improperly configured or physically unsecured PBXs and computerized telephone systems (CTS) can allow interception of sensitive voice communications.

The risks that these vulnerabilities present justify the policy restricting the use of telephones. The basic telephony concepts behind these vulnerabilities are beyond the scope of this document. Restricting the use of desktop equipment (e.g., cordless telephones, speakerphones, answering devices, call forwarding options, etc.) in areas where sensitive information will be discussed mitigates some of the risks associated with these vulnerabilities. Following the procedures and guidance in NIST SP 800-24, "PBX Vulnerability Analysis: Finding Holes in Your PBX before Someone Else Does," will mitigate others. Finally, where telephones must be used to discuss sensitive information, additional guidance can be obtained from the NSA and DOD regarding telephone models that reduce or eliminate the vulnerabilities listed in this section.

4.4.3 Voice Mail

Sensitive information is not to be stored on voice mail systems. Since secure email is available, voice mail should be authorized only by exception for personnel whose responsibilities require it.

Since it is possible to perform traffic analysis or denial of service attacks on telephone systems by abusing voice mail, any user of voice mail should enable password protection for voice mail access. Voice mail passwords should have no fewer than four (4) characters, and no consecutively repeated characters. Passwords should be changed at least every ninety (90) days.

Voice mail responsibilities are provided in the following table.

Voice Mail Responsibilities
ISSOs
Identify the personnel or position(s) responsible for telephone usage in the applicable voice communications policy statement
PBX Administrators
Identify the personnel or position(s) responsible for telephone usage in the applicable voice communications policy statement
Ensure that telephone systems are configured to enable enforcement of minimum password requirements for voice mail
Telephone Users
Create secure passwords that adhere to at least the minimum voice mail password requirements

4.5 Data Communications

This section addresses vulnerabilities inherent in data communications and the operational controls needed to mitigate the risks associated with those vulnerabilities. Data communications include telecommunications, video teleconferencing, and voice over data network technology.

4.5.1 Telecommunications Protection Techniques

Extreme caution should be exercised when telecommunications protection techniques are being considered as alternatives to the use of encryption. While such technologies may represent a lower-cost approach, their ability to protect information may not provide an adequate level of protection. During the procurement process, emphasis must be placed on the effectiveness of the tool or approach selected.

Except in low impact cases, establish alternate telecommunications services including necessary agreements to permit the resumption of specified operations for essential missions and business functions within a Component-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites

Telecommunications protection responsibilities are provided in the following table.

Telecommunications Protection Responsibilities
Component CISO/ISSMs
Advise DHS Project Managers on the selection of telecommunications protection techniques that could serve as an alternative to encryption for data transmission protection techniques
System Owners
Select the telecommunications protection techniques that meet their security needs and are consistent with DHS security policies and most cost-effective.

Although sensitive data may be contained entirely within a protected network, there still exists the possibility that a disgruntled, malicious, or subversive individual may be able to access sensitive data by means of devices or software that capture data traveling across the network. This is often accomplished by sniffing software, which uses low-level driver commands to put a Network Interface Card (NIC) into promiscuous mode. Normally, network interface cards only accept information directed to them and ignore information that does not have their address. A promiscuous NIC collects all information from the network to which it is attached, regardless of the intended address.

Tools for detecting NICs that are in a promiscuous mode are available. The scanning of systems referred to in Section 5.4.8, "Testing and Vulnerability Management," can detect software programs that are capable of enabling this mode. Scanning tools can also detect software operating in promiscuous mode when it is collecting data from a NIC.

A malicious individual can make information unavailable by rendering the network unusable. This is commonly known as a denial of service (DoS) attack. An individual can initiate a DoS attack by broadcasting large amounts of data, by physically compromising network elements, or by taking advantage of some of the inherent weaknesses of the TCP/IP handshaking process.

Intrusion detection system tools exist that can detect most types of DoS attacks (see Section 5.4.4, "Firewalls"). Proper configuration of server systems can also mitigate these attacks by altering the default TCP/IP software configuration settings.

Additional vulnerabilities exist with respect to the accuracy of the information transmitted. There is a class of attacks known as "man in the middle." In these attacks, an individual receives information, alters it, and transmits the altered information to its originally intended recipient in such a manner that the recipient believes that the information was sent directly from the original destination. These attacks can be mitigated through the use of message digests. Message digests calculate a fixed length value from any amount of text. This fixed length value is very difficult to reproduce. Also, encryption and digital signing make the task of altering data difficult or sufficiently time consuming that it is of little use.

NIST SP 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network,* outlines these and other security considerations involving telecommunications. NIST contends that 65 percent of the compromises regarding availability, integrity and privacy/ confidentiality are committed by employees through errors, omissions, and malicious acts.

Establishment by Components of alternate telecommunications services is required by DHS Sensitive Systems Policy Directive 4300A, Section 4.5.1.

4.5.2 Facsimiles

Facsimile (fax) technology was developed for scanning and transmitting documents. Although fax is traditionally a telephony-based application, the technology has evolved to address the transmission of text or image files.

Fax inherently is not a secure means of communication, and faxes can easily be intercepted and decoded. Fax protocols provide neither authentication nor non-repudiation services, which allows fax traffic to be sent to or received by unintended recipients. The commonly used Group III fax protocol implements support for proprietary and undocumented data exchange using a feature called nonstandard facilities (NSF). Fax servers or fax modems attached to networks provide a potential means for network intrusion and penetration.

Several proactive steps must be taken to ensure adherence to DHS fax policy. This policy is designed to prevent unauthorized paths into the protected network, commonly referred to as "backdoors." For example, "fax polling" features must be disabled. Fax polling allows a remote fax machine to access a fax machine and retrieve any data in memory waiting to be delivered.

Any fax machine used to transmit sensitive information should be placed in a locked room that only trusted individuals are able to access. The fax machine should also be placed in such a fashion that any documents being sent or retrieved are not visible to non-trusted individuals.

Anyone sending sensitive information should verify the recipient's secure fax number immediately before sending and should ascertain whether or not the intended recipient (or trusted subordinate) will be present to receive the fax as soon as it is sent.

Sensitive information should never be sent to an unattended fax machine. Fax machines should have the "memory" features turned off, so that the information cannot be accessed or retransmitted (possibly to an unauthorized recipient) at a later time.

All documents being transmitted should be appropriately labeled (see Sections 4.3.2 and 4.11 of this handbook). The reverse procedure should be used if the individual is receiving. All documents transmitted or received should be immediately removed from the fax machine room and appropriately stored.

Extremely sensitive or classified faxes require more stringent controls, such as transmission over trusted links (as opposed to the Public Switched Telephone Network (PSTN)). If such a fax must be sent via the PSTN, use of encryption devices is required.

Because a fax machine is operated in a similar manner to a copying machine, transmission of extremely sensitive or classified data should be followed by using the machine in copier mode to process several copies of a test pattern or some unclassified data to remove the image of the sensitive data from the fax machine's imaging apparatus.

Facsimile responsibilities are provided in the following table.

Facsimile Responsibilities
CISO
Establishes and enforces policy relating to the use of facsimile machines
System/Network Administrators
Ensure that facsimile machines connected to DHS resources are protected and configured to prevent mishandling of sensitive information
Facility Managers
Ensure that appropriate physical security requirements are implemented for facsimile machines
ISSOs
Ensure that applicable information security requirements are applied as necessary to facsimile machines
Ensure that the SP addresses facsimile machines connected to systems

4.5.3 Video Teleconferencing

Video teleconferencing permits DHS personnel to engage in live exchanges of information without the lost time and high cost of traveling to attend a face-to-face meeting in a distant city. Video teleconferencing offers many beneficial applications, including training and distance learning, data collaboration, large and small meetings, and informational broadcasts.

Two basic mechanisms allow video teleconferencing to take place. The most basic uses professional quality video equipment, which displays remotely on television monitors or similar projection devices. The second uses inexpensive video devices, which are attached to computers and display on computer screens using protocols such as H.323 over IP networks. The transmission medium for both can be within a protected network, across the PSTN or across an internal or external (Internet) network connection.

The first approach allows the equipment to be controlled, operated, and secured by trusted individuals with specific responsibilities for the teleconferencing equipment. Operators can assure that any recording of information is labeled and secured according to its sensitivity (see Section 4.3.2), properly disposed of when no longer useful (see Section 4.3.3), and secured during transmission by use of proper encryption (see Section 5.5.1) or tunneling. They can also confirm that the broadcast information is being sent to the proper location. It is recommended that, to the degree possible, such conferences occur in a point-to-point manner between two sites.

The second approach is not authorized. This technology introduces all of the vulnerabilities associated with sensitive data transmission across an IP network (see Section 4.5.1 of this handbook), as well as the vulnerabilities associated with other devices, which may unwittingly make sensitive data available to unauthorized parties (see Sections 4.4.2 and 4.6.3). The ability of an individual to easily eavesdrop on such communications or record them on media for improper dissemination is an unnecessary risk.

The design of the video teleconferencing system and facility must be approved by the DHS CISO before purchase and installation. Components must develop standard operating procedures for the operations and maintenance of this capability. These procedures must specify that:

- All participants must have the appropriate clearance and need-to-know
- Video conferencing must be disabled when not in use
- Any videotapes created of the teleconference must be appropriately labeled with the highest classification of the information contained on the videotape and secured in accordance with established media controls

Video teleconferencing responsibilities are provided in the following table.

Video Teleconferencing Responsibilities
AOs Carefully weigh the risk associated with the use of video teleconferencing equipment connected to DHS systems prior to authorizing **Component CISOs/ISSMs**

Video Teleconferencing Responsibilities
Advise DHS personnel on the selection and secure use of video teleconferencing technologies
Supervisors
Establish procedures to ensure that only authorized attendees participate in teleconferencing sessions
Ensure that procedures are in place to disable video teleconferencing equipment when not in use
Ensure that procedures are in place to label and store videotapes recorded during the teleconferencing
ISSOs/Teleconferencing Operators
Ensure that video teleconferencing is addressed in the SP if the equipment is connected to a DHS system
Ensure that video teleconferencing equipment is disabled and secure when not in use
Ensure that appropriate transmission protections are in place commensurate with the highest sensitivity of information to be discussed when conducting a video teleconferencing session
Users
Do not discuss information during a teleconferencing session at a higher level of classification than that established for the conference

4.5.4 Voice over Data Networks

Voice over Internet Protocol (VoIP) and similar technologies move voice over digital networks. These technologies use protocols originally designed for data networking. Such technologies include Voice over Frame Relay, Voice over Asynchronous Transfer Mode, and Voice over Digital Subscriber Line (refer to NIST SP 800-58 for further information).

Voice over data networking cannot yet be considered a mature technology. Although various standards are currently being published, there is little assurance that systems that incorporate these capabilities can be adequately protected. Moreover, there are hidden costs associated with their use that make their implementation suspect on technical grounds other than security considerations. These include interoperability issues. Although not prohibited, implementation of these technologies is discouraged.

Prior to implementing voice over data network technology, Components must conduct rigorous risk assessments and security testing and provide Department business justification for their use. Furthermore, any systems that employ this technology must be authorized for use with residual risks clearly identified.

Redundancy can be accomplished by establishing major (trunk) links in a load balancing fashion. This concept involves having multiple pathways that appear to be a single pathway in terms of addressing or routing. If one of the alternate pathways fails, the share of traffic that it was handling is distributed to the other pathways. If there is only one other pathway, the situation is known as fail over. Such a failure should show an indication on the network monitoring tools. Technicians could then be dispatched to repair the failed element and return the link to full operation.

Information integrity is a significant security concern when using voice over data networks. Services provided by commercial entities are not directly controlled by DHS staff. Encryption of any data (including voice) that traverses these links is mandatory. The contractual arrangements

with these suppliers must specify that only U.S. Citizens are involved in the maintenance and operation of these links.

Authentication controls and audit logging may be provided by the same technologies that provide these capabilities for digital data traffic. VoIP standards also include specification of a Media Gateway Control Protocol (MGCP) that also collects audit information.

As with many technologies, there are numerous vendor-specific protocols and numerous standards in development. Many of the security issues related to VoIP are dependent upon vendor selection and architecture design. Rigorous testing and clear business justification should be completed before any AO approves the use of this technology.

Responsibilities related to voice over data networks are provided in the following table.

Voice Over Data Networks Responsibilities
Project Managers
Ensure the design of voice over data network implementations have sufficient redundancy to ensure network outages do not result in the loss of both voice and data communications
Ensure appropriate identification and authentication controls, audit logging, and integrity controls are implemented on every element of their voice over data networks
ISSOs
Ensure that the inherent risks of voice over data network technology are clearly identified in the Authorization Package to include the business justification for their use
Ensure that physical access to voice over data network elements is restricted to authorized personnel
Ensure that appropriate identification and authentication controls, audit logging, and integrity controls are implemented on every element of their voice over data networks
Ensure that auditing is enabled and audit logs are reviewed on a regular basis
Ensure that systems that employ VoIP technology have been authorized for this purpose with residual risks clearly identified and addressed in the Authorization Package
Network/System Administrators
Ensure that appropriate identification and authentication controls, audit logging, and integrity controls are properly configured on every element of their voice over data networks
Facility Managers
Ensure that physical access to voice over data network elements is restricted to authorized personnel

4.6 Wireless Network Communications

Wireless network communications technologies include the following:

- Wireless systems (e.g., wireless local area networks [WLAN], wireless wide area networks [WWAN], wireless personal area networks [WPAN], peer-to-peer wireless networks, information systems that leverage commercial wireless services). Wireless systems include the transmission medium, stationary integrated devices, firmware, supporting services, and protocols

- Wireless mobile devices capable of storing, processing, or transmitting sensitive information (e.g., PDAs, smart telephones, two-way pagers, handheld radios, cellular telephones, personal communications services [PCS] devices, multifunctional wireless devices, portable audio/video recording devices with wireless capability, scanning devices, messaging devices)
- Wireless tactical systems, including mission-critical communication systems and devices (e.g., include Land Mobile Radio [LMR] subscriber devices and infrastructure equipment, remote sensors, technical investigative communications systems)
- Radio Frequency Identification (RFID)

General guidelines pertaining to all wireless communications technologies are provided in this section. Policies more specific to wireless systems, wireless mobile devices, wireless tactical systems, and RFID are provided in Sections 4.6.1, 4.6.2, 4.6.3, and 4.6.4, respectively.

Components employing encryption on wireless technologies must implement and enforce a key management plan consistent with DHS Public Key Infrastructure (PKI) Policy Authority. The key management plan must clearly define the practices, procedures, and techniques used to enforce the key management policy and functional requirements. Representative guidance may be drawn from NIST SP 800-57, "Recommendation for Key Management – Part 2: Best Practices for Key Management Organization".

For wireless technologies classified as general support systems or major applications, the key management plan must be addressed in the SP.

Wireless communications responsibilities are provided in the following table.

Wireless Communications Responsibilities
PKI Policy Authority
Establishes and enforces the security requirements detailed in the key management plan
AOs
Specifically approve or prohibit the use of wireless communications technologies within the Department
Approve the implementation and use of the key management plan at acceptable risk levels
Ensure that appropriate and effective security measures are included in the key management plan
Approve migration plans for transitioning legacy wireless systems
Component CISOs/ISSMs
Advise System Owners and Project Managers concerning implementation of key management plans
Enforce DHS key management policy and procedures
ISSOs
Ensure that key management security controls and functional requirements are implemented
Ensure that security assessments are conducted to evaluate the effectiveness of security objectives and controls supported by the key management plan
System/Network Administrators

Wireless Communications Responsibilities
Implement and enforce technical security mechanisms specified in key management plan
DHS Managers, Supervisors, and Employees
Adhere to DHS policy concerning the use of wireless communications technologies
Adhere to DHS policy concerning key management policy and procedures
DHS CISO
Review waivers pertaining to wireless systems policy

4.6.1 Wireless Systems

Wireless system policy and procedures are described more completely in Attachment Q1 (*Wireless Systems*) to This Handbook.

Wireless systems allow mobile devices, wired devices, and other devices to process, store, or transmit sensitive information using radio frequency (RF) or infrared (IR) capabilities. Wireless systems are vulnerable to a number of traditional attacks and to attacks specific to wireless technologies. These attacks fall into the following categories:

- Unauthorized access
- Denial-of-service/jamming/interference
- Signal detection/eavesdropping
- Spoofing/masquerading
- Message modification

Use of appropriate countermeasures will help ensure that wireless systems comply with DHS information security policy.

This Handbook's Attachment Q1, *Wireless Systems*, provides implementation guidance for developing and implementing security for wireless systems.

Wireless system responsibilities are provided in the following table.

Wireless System Responsibilities
AOs
Approve the use of standards-based wireless system technologies
Approve the implementation and use of wireless systems at a specified risk level during the Security Authorization Process
Ensure that appropriate and effective security measures are included in the SP
Component CISOs/ISSMs
Advise System Owners and Project Managers concerning the implementation of wireless technologies
Enforce DHS wireless systems policy

Wireless System Responsibilities
Enforce DHS policy concerning the reporting requirements for wireless security vulnerability assessments
System Owners/Project Managers
Develop risk mitigation plans for prioritizing corrective actions and implementation milestones
Develop migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless systems to DHS-compliant security architectures
ISSOs
Ensure that wireless systems security controls are properly implemented and configured and are addressed in the SP
Ensure that routine security assessments of wireless systems identify unauthorized wireless devices, backdoors, and other system vulnerabilities, and enumerate vulnerabilities, risk statements, risk levels, and corrective actions
Implement risk mitigation plans for prioritizing corrective actions and achieving implementation milestones
Implement migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless systems to DHS-compliant security architectures
System/Network Administrators
Ensure that wireless system security controls are properly implemented and configured in accordance with the SP
Ensure that routine security assessments are accomplished on wireless systems to identify rogue access points, backdoors, and other system vulnerabilities, and to enumerate vulnerabilities, risk statements, risk levels, and corrective actions
DHS Managers, Supervisors, and Employees
Adhere to DHS policy concerning the use of wireless systems to process, store, or transmit sensitive information
Adhere to DHS policy concerning the use of wireless systems in areas where sensitive information is being discussed

4.6.2 Wireless Mobile Devices

Wireless mobile devices include any wireless clients capable of storing, processing, or transmitting sensitive information.

Guidance applicable to wireless mobile devices is detailed in this Handbook's Attachment Q2, "Mobile Devices."

There is currently no DHS-approved encryption software for wireless mobile devices, although individual Components may be using products that provide adequate protection. As DHS or NSA standards are established, they will be discussed in this section of the Handbook.

Personally owned mobile devices are not authorized for processing, transmitting, or storing sensitive or classified information. Personally owned mobile devices may not be connected to sensitive or classified systems or networks.

Government-owned mobile devices may be used in conjunction with Department networks or systems (to include any downloading of data from a user's workstation to these devices) only if the current Security Authorization Process documentation (available on the Compliance and Technology page on DHS Connect) specifically addresses the inherent risks associated with their use and the AO evaluates and accepts any residual risk. Re-authorization is required if these issues are not addressed in the most current Security Authorization Process documentation.

System Owners and Project Managers must identify and implement as many countermeasures as appropriate to strengthen the security of wireless devices. These countermeasures include the use of passwords, personal firewalls, and antivirus software; the monitoring of malicious activities; the use of modification detection software and of software that will allow the device to dynamically identify and adapt to each wireless mode of operation; the tracking of data and assets; and management protocols. Countermeasures should allow the system administrator to maintain a user and community profile through unit identification and validation, which would in turn allow administrators to remove data, update software, and log and track unauthorized removal where appropriate.

Because of their portability and mobility, mobile devices are also extremely susceptible to theft, physical damage, and loss—all of which could lead to compromise of information.

Components must develop and maintain a property inventory list of all wireless devices authorized for use. This list includes serial numbers and/or seat numbers, user names, use, and location of all mobile devices for accountability purposes. Each DHS-owned mobile device is required to have an asset tag whose number is included in the inventory list. Rules of Behavior for mobile devices must be published and enforced. This Handbook's Attachment G, *Rules of Behavior* provides guidance on developing Rules of Behavior, including rules for mobile devices.

This Handbook's Attachment Q2, "Mobile Devices" provides guidance for developing and implementing wireless security.

Wireless portable electronic device responsibilities are provided in the following table.

Wireless Device Responsibilities
AOs
Approve the use of Government-owned, DHS-approved wireless devices and accessories used to connect with, process, store, or transmit sensitive information
Ensure that appropriate and effective security measures are included in the SP
Authorize the use of Government-owned wireless devices and accessories in areas where sensitive information is discussed
Evaluate the risk associated with authorizing wireless devices to connect with, process, store, transmit, or access sensitive information and systems during the Security Authorization Process

Wireless Device Responsibilities
Approve or disapprove the use of mobile code (e.g., ActiveX)
System Owners/Project Managers
Develop risk mitigation plans for prioritizing corrective actions and implementation milestones
Develop migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless devices to DHS-compliant security architectures
Maintain an inventory of all approved wireless devices in operation
Component CISOs/ISSMs
Enforce DHS policy on the use of wireless devices and accessories in areas where sensitive information is discussed
Enforce DHS policy concerning the use of wireless devices and accessories to connect with, store, process, or transmit combinations, PINs, or sensitive information
Develop procedures for implementation of strong identification, authentication, data encryption, and transmission encryption for wireless devices to protect sensitive information from compromise
Enforce DHS policy concerning the use of mobile code and antivirus software on wireless devices
Identify and establish cost-effective countermeasures to denial-of-service attacks for wireless devices
ISSOs
Ensure that wireless devices are not permitted in areas where sensitive information is discussed unless authorized in writing by the AO
Enforce DHS policy concerning the use of wireless devices to process, store, or transmit sensitive information
Enforce DHS policy concerning the use of mobile code and antivirus software on wireless devices
Implement cost-effective countermeasures to denial-of-service attacks for wireless devices
Ensure that all wireless devices that are to be reused or declared surplus, disposed of, recycled, or returned to the owner or manufacturer are sanitized. (see Section 4.3.3 of this handbook for approved procedures)
Implement migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless devices to DHS-compliant security architectures
Enforce prohibition of add-on devices such as cameras and recorders
System/Network Administrators
Ensure that wireless device security controls are properly implemented and configured in accordance with the SP
Ensure that routine security assessments are accomplished on wireless devices
DHS Managers, Supervisors, and Employees
Adhere to DHS policy concerning the use of wireless devices in areas where sensitive information is being discussed
Adhere to DHS policy concerning the use of wireless devices to process, store, transmit, or access

Wireless Device Responsibilities
combinations, PINs, or sensitive information

4.6.2.1 Cellular Phones

Cellular phones used in areas where sensitive information is discussed have the same inherent vulnerabilities as cordless telephones and speakerphones as discussed in Section 4.4.2 of this handbook. They potentially allow a discussion being held in the same area to be overheard by a third party.

As with traditional telephones, cellular communications can be intercepted. While the interception of conversations over telephones requires insertion of a monitoring device; the interception of cellular communications does not, and information transmitted by cellular phones can be intercepted at reasonably great distances. Cellular phone credentials can be cloned to other phones, allowing the cloned phone to masquerade as the original phone and allow covert monitoring of conversations.

Cellular phone responsibilities are provided in the following table.

Cellular Phone Responsibilities
Managers Ensure that employees are aware of DHS policy prohibiting the discussion of sensitive information while using a wireless telephone
Users Ensure that sensitive information is not discussed while using a wireless telephone

4.6.2.2 Pagers

Text messages may be sent via text pagers, from a cellular service provider's Web page, or from other Web sites that allow users to send text messages. Pagers have the same inherent vulnerabilities as cellular phones with respect to exposure of sensitive information to unauthorized recipients (see Section 4.6.2.1).

Text messages rely on the service provider's network and are not encrypted. There is thus no assurance of the security of these services. Moreover, text-message devices can be spammed until the user's mailbox is full.

Pagers must not be used to transmit sensitive or classified information that is explicitly labeled as sensitive or classified, nor should they be used to transmit information on computer or network problems or status. This information could be intercepted and used to identify the configuration and possibly the location of information systems.

A preferred alternative to transmitting text messages is to page an individual with a phone number and require the individual to call that number using a landline (not cellular or mobile) telephone from a location where the conversation could not be overheard by non-trusted persons.

Pager responsibilities are provided in the following table.

Pager Responsibilities
Managers
Ensure that employees are aware of DHS policy prohibiting the transmission of sensitive information to pagers
Users
Ensure that sensitive information is not transmitted to pagers

4.6.2.3 Multifunctional Wireless Devices

Wireless devices have evolved to be multifunctional (cell phones, pagers, and radios can surf the Internet, retrieve email, take and transmit pictures). Most of these functions do not have sufficient security.

Where there is a strong business justification for their use, DHS-owned wireless devices can be equipped to allow synchronization with approved Department owned computers. Data is encrypted or decrypted, as needed, for synchronization with computer-based personal information managers (PIMs) and other programs.

The risk assessment for multifunctional wireless devices must in all cases include an assessment of the risks associated with all functions, including infrared (IR), radio frequency (RF), and video. The AO may allow the use of multifunctional wireless devices based on the sensitivity and classification of the data and the associated risks.

Use of peripheral devices must be tightly controlled. Audio and video recording capabilities should be prohibited unless specifically required for an individual's duties. Unauthorized recording of sensitive conversations or images of sensitive equipment could be used to compromise the security of DHS systems.

Multifunctional wireless device responsibilities are in the following table.

Multifunctional Wireless Device Responsibilities
AOs
Approve the implementation of multifunctional wireless devices at an acceptable level of risk
Ensure prior to authorization that the SP adequately addresses the protection of sensitive material accessed and stored on multifunctional wireless devices.
Project Managers/System Owners
Ensure that security requirements for multifunctional wireless devices are communicated to the Project Manager and system administrators
System/ Network Administrators
Ensure that multifunctional wireless devices are configured properly with encryption enabled to prevent unauthorized access, disclosure, damage, modification, or destruction of data
Ensure that multifunctional wireless devices are periodically scanned for rogue access points and other vulnerabilities

Multifunctional Wireless Device Responsibilities
ISSOs
Ensure that the SP addresses the protection of sensitive material accessed and stored on wireless devices
Ensure that security requirements for multifunctional wireless devices are addressed in the SP and Rules of Behavior
Ensure that routine security assessments are accomplished for multifunctional wireless devices to identify rogue access points, backdoors, and other system vulnerabilities, and to enumerate vulnerabilities, risk statements, risk levels, and corrective actions

4.6.3 Wireless Tactical Systems

Wireless tactical systems include Land Mobile Radio (LMR) subscriber devices, infrastructure equipment, remote sensors, and technical investigative communications systems. Because they are often deployed under circumstances in which officer safety and mission success are at stake, wireless tactical systems require even greater security measures. To ensure secure tactical communications, Components must implement strong identification, authentication, and encryption protocols designed specifically for each wireless tactical system.

Wireless tactical system policy and procedures are described more completely in Attachment Q3, *Wireless Tactical Systems* to this Handbook.

Wireless tactical communications systems are also subject to issues such as technology advances, standards, and functional convergence. As the use of wireless tactical communications systems evolves, Components must develop and implement plans for migration to the new technologies. AOs must ensure that these migration plans are consistent with DHS policy and that appropriate waivers have been obtained.

LMR systems are the primary means of wireless communications for several Components. Security and risk management principles must be included in every phase of the LMR system development lifecycle. LMR network communications traffic should include encryption and security controls such as those specified by FIPS 140-2, *Security Requirements for Cryptographic Modules*, and FIPS 197, *Advanced Encryption Standard (AES).*

LMR subscriber units can periodically update and rekey encryption protocols manually by using a handheld key variable loader (KVL) or automatically via over-the-air-rekeying (OTAR) techniques. With OTAR technology, radios can be rekeyed within seconds over the air from a remote location, allowing for easier and more regular rekeying, and resulting in improved security. In addition, the OTAR channel can be used for digital voice transmissions in the encrypted mode for emergency interoperability.

LMR security and policy guidelines and standards defined by Project 25 (P25) should be implemented where appropriate. The primary objectives of the P25 standards are to promote interoperability among digital or analog LMR equipment used by various levels of Government, support backward compatibility with legacy LMRs, enhance spectrum efficiency, and maximize economies of scale. All DHS LMRs must be built on P25-compliant platforms or be capable of interfacing with P25-compliant platforms to ensure that DHS requirements can be satisfied in a timely manner. Waivers to this requirement must be approved by the DHS CISO.

This Handbook's Attachment Q3, *Wireless Tactical Systems*, provides guidance for developing and implementing wireless tactical system security.

Wireless tactical system responsibilities are provided in the following table.

Wireless Tactical System Responsibilities
AOs
Approve the use of wireless tactical systems technologies
Approve the implementation and use of wireless tactical systems to process, store, or transmit sensitive information at acceptable risk levels
Ensure security measures are included in the SP
Evaluate and submit waivers to the DHS CISO for wireless tactical systems when compliance with DHS information security policy could potentially compromise tactical investigations, endanger personnel safety, or put the public at risk
System Owners/Project Managers
Implement cost-effective security measures specified in the SP including strong identification, authentication, and encryption
Ensure that the AO is immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents
Ensure allocation of resources to support security requirements and enforcement controls specified in the SP
Ensure that tactical wireless communication security requirements are communicated to ISSOs and system administrators
Develop and implement migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless tactical systems to DHS-compliant security architectures
Maintain an inventory of all wireless tactical systems used to process, store, and transmit sensitive information
Ensure all LMR systems comply with Project 25 (P25, EIA/TIA-102) security standards where applicable
Component CISOs/ISSMs
Enforce DHS policy concerning the use of tactical communication systems to process, store, transmit, or access sensitive information
Develop and enforce DHS policy concerning mitigation measures for DoS attacks
Enforce LMR system compliance with Project 25 (P25, EIA/TIA-102) security standards
ISSOs
Ensure that the AO is immediately notified whenever any security features are disabled in response to time-sensitive, mission-critical incidents
Implement DHS policy concerning the use of tactical communication devices to process, store, transmit, or access sensitive information
Ensure that any tactical communication devices used to process sensitive information are not permitted

Wireless Tactical System Responsibilities
in conference rooms or secure facilities where sensitive information is discussed without written authorization from the AO Perform security assessments and validate the security posture of LMR subscriber units via OTAR or hard rekeying using a crypto-period no longer than one-hundred and eighty (180) days Ensure that all information is cleared from wireless tactical systems that are to be reused or surplussed Ensure that wireless tactical systems are sanitized prior to being disposed of, recycled, or returned to the owner or manufacturer (see Section 4.3.3, for approved procedures) **DHS Managers / Supervisors** Ensure that the AO is immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents Ensure employees are aware of DHS policy and procedure for discussing sensitive information while using tactical communication devices **Employees** Adhere to DHS policy and procedures concerning the use of tactical communication devices that access, process, store, or transmit sensitive information and systems

4.6.4 Radio Frequency Identification

RFID enables wireless identification of objects over significant distances. Because of the computing limitations of RFID tags, it often is not feasible to implement many of the security mechanisms such as cryptography and strong authentication, that are commonly supported on personal workstations, servers, and network infrastructure devices. RFID security controls can support Departmental and Component privacy objectives, mitigate risks to business processes, and prevent the disclosure of sensitive data.

RFID policy and procedures are described more completely in *"Sensitive RFID Systems,"* Attachment Q4 to the *DHS 4300A Sensitive Systems Handbook*.

4.7 Overseas Communications

Communication outside of the United States or its territories has different security requirements than domestic communication. The Department of State has published a series of Foreign Affairs Manuals relevant to these requirements.

Wireless communications are highly vulnerable to interception and monitoring. DHS employees overseas must be informed of the risks and the appropriate precautions they should follow when using wireless devices overseas. Use of secure wireless devices overseas must be approved by the DHS CISO.

The following sections of Volume 12 of the U.S. Department of State *Foreign Affairs Manual* (FAM), found at http://www.state.gov/m/a/dir/regs/fam/12fam/index.htm, contain information relevant to overseas communication:

12 FAM 610, *Organization and Purpose of Computer Security (COMPUSEC)*
12 FAM 620, *Unclassified Automated Information Systems*

12 FAM 630, *Classified Automated Information Systems*
12 FAM 640, *Domestic and Overseas Automated Information Systems Connectivity*
12 FAM 650, I *Components*
12 FAM 660, *Communications Security* (this section has been designated Sensitive—NOFORN and is not available via the Internet; contact the Department of State to obtain a hardcopy version).

Overseas communications responsibilities are provided in the following table.

Overseas Communications Responsibilities
DHS CISO
Establishes and enforces policy relating to overseas communications
Component CISOs/ISSMs
Ensure that Component information systems under their purview comply with Department of State 12 FAM 600 *Information Security Technology*, for systems that communicate with overseas locations
Project Managers/System Owners
Ensure information systems under their control or under development that will communicate with overseas locations comply with the requirements of Department of State 12 FAM 600, *Information Security Technology*
System/Network Administrators
Ensure that information systems under their control that will communicate with overseas locations are properly configured and maintained to comply with the requirements of Department of State 12 FAM 600, *Information Security Technology*
ISSOs
Ensure that information systems under their control that communicate with overseas locations comply with Department of State 12 FAM 600, *Information Security Technology*

4.8 Equipment

Equipment security encompasses workstations, laptops, other mobile computing devices, personally owned equipment, and the maintenance of these items. This section addresses the use and maintenance of computer equipment and stresses the importance of individual accountability in protecting these resources.

System administrators and ISSOs must ensure that all users are educated in the proper procedures for logging off and for configuring screen savers. Specific procedures for logging off, locking workstations, and enabling password-protected screensavers are published in Attachment I to this Handbook, "Workstation Logon."

The following guidelines apply to the protection of workstations used to process or store sensitive information:

- Workstations must be adequately protected from theft.
- Only licensed and approved operating systems and applications may be used on DHS workstations.

- All default vendor or factory-set administrator accounts and passwords must be changed before installation or use.
- All equipment is to be marked with the highest level of classification of information that has ever been processed or stored on the device, if there are any devices authorized for processing National Security information in the vicinity.
- Equipment must be housed in facilities authorized to process sensitive information.

4.8.1 Workstations

All users must be instructed to log off or lock their workstation any time the workstation is left unattended. As an added precaution, users should also use a password-protected screensaver. The screensaver should activate after no more than fifteen (15) minutes of inactivity.

Workstation responsibilities are provided in the following table.

Workstation Responsibilities
Facility Managers
Ensure that physical security measures are adequate to protect computers (PCs, laptops, and servers) from theft
Site Security Staff/ISSOs/Supervisors
Enforce DHS policy on securing workstations when unattended by users
System/Network Administrators
Ensure where possible that workstations are configured for automatic logoff, or with automatic screensaver activation after 5 minutes of inactivity
Users
Adhere to DHS policy by securing workstations when unattended

4.8.2 Laptop Computers and Other Mobile Computing Devices

DHS relies heavily on laptop computers and other mobile computing devices. The mobility of these devices has increased the productivity of the workforce, but at the same time, mobility has increased the risk of theft and unauthorized data disclosure. It is important to employ additional measures to protect these resources including laptops and other mobile computing devices and the data they store and process.

The increased risk of theft of laptop computers and other mobile computing devices presents both security and cost concerns. Both hardware replacement and restoration of data entail significant cost. The risk of data disclosure is also a major security concern. Care must be taken to guard against theft at all times, and fundamental security principles must be observed with mobile computing devices. For example, the user's password should never be written down and stored with the device.

Mobile computing devices cannot be connected to DHS networks or systems unless such connections are authorized to the network or system. The security plan must identify the devices that can be used to access the network or system, the purposes for the access, and the security controls to be employed for the connection. Any laptop computers or other mobile computing

devices that process sensitive data (whether or not they are connected to a DHS network) must employ virus protection. All removable media must be scanned prior to use to ensure it is free of malware.

Rules of Behavior for mobile computing devices must be published and enforced. This Handbook's Attachment G, "Rules of Behavior" provides guidance on developing Rules of Behavior.

Mobile computing devices that process sensitive data must employ encryption technology. Encryption policies and procedures are addressed in Section 5.5.1 of this handbook.

Responsibilities related to mobile computing devices are provided in the following table.

Laptop Computer and Other Mobile Computing Device Responsibilities
DHS CISO
Establishes DHS policy regarding the use of mobile computing devices
Component CISOs/ISSMs
Enforce DHS policy regarding the use of mobile computing devices
Provide technical expertise and evaluate the effectiveness of encryption methods for mobile computing devices
System/Network Administrators
Provide technical expertise and evaluate the effectiveness of encryption methods for mobile computing devices
Ensure that encryption technology is installed and properly configured on mobile computing devices
Assist ISSOs in implementing technical requirements for mobile computing devices
ISSOs
Ensure that security of mobile computing devices is adequately addressed in the security plan
Ensure users are aware of their responsibility to adhere to the Rules of Behavior for mobile computing devices
Ensure that users are trained in the use of encryption for mobile computing devices
Ensure that physical security controls are in place for mobile computing devices
Ensure the unique requirements for connection of mobile computing devices to the network are addressed in the Security Plan
Ensure that encryption methods employed on mobile computing devices provide the protection required in the security plan
Users
Obtain written approval of the office director before taking mobile computing device overseas
Comply with the Rules of Behavior for mobile computing devices
Utilize encryption technology provided for mobile computing devices
Physically secure mobile computing devices when not in use

Laptop Computer and Other Mobile Computing Device Responsibilities
Read and adhere to the mobile computing device policies and procedures in this section and in Rules of Behavior
Make supervisors and managers aware of any problems encountered in implementing mobile computing device guidance and procedures

4.8.3 Personally Owned Equipment and Software

Users must not use personally owned equipment (e.g., laptop computers, cell phones, and media) or software to process, access, or store sensitive information. Also prohibited are USB flash (thumb) drives, external drives, and diskettes. Exceptions 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 systems' Security Authorization Process.

Components are 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.

Policy and guidance pertaining to the protection and disposal of personally owned equipment and software is addressed in Section 4.3 of this handbook. Components are required to ensure that policies are reflected in appropriate Rules of Behavior documents and reinforced during periodic security awareness sessions.

Responsibilities related to personally owned equipment and software are provided in the following table.

Personally Owned Equipment and Software Responsibilities
AOs
Carefully evaluate the risk associated with authorizing the use of personally owned equipment or software
Component CISOs/ISSMs
Enforce DHS policy prohibiting the use of personally owned equipment to connect, process, store, or access sensitive information and systems
ISSOs
Enforce DHS 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

Personally Owned Equipment and Software Responsibilities
Users
Adhere to DHS policies prohibiting the use of personally owned equipment and software

4.8.4 Hardware and Software

Components must be cognizant of the threats, vulnerabilities, and risks associated with hardware and software installation and maintenance on DHS systems.

The DHS CISO has published secure baseline configuration guides for several operating systems, the Oracle 9i database management system, and CISCO routers, and will provide additional configuration guides as required. These hardening guides provide system and database administrators with a clear, concise set of procedures that ensure a minimum baseline of security in the installation and configuration of the hardware and software.

Baselines were developed using a variety of security guidelines from the NSA, the Defense Information Systems Agency (DISA), NIST and other Federal agencies, and from vendor recommendations. The principle reference used was NIST SP 800-70: "Security Configuration Checklists Program for Information Technology (IT) Products – Guidance for Checklists Users and Developers."). These baselines represent the minimum configuration requirements; Components are authorized to implement more rigorous configuration guides. If unable to meet the published configuration baselines, a waiver or exception is required.

Hardware and software responsibilities are provided in the following table.

Hardware and Software Responsibilities
DHS CISO
Approves secure baseline configuration guides
Component CISO/ISSMs
Provide guidance in the preparation of secure baseline configuration guides for hardware and software; DHS CISO approves secure baseline configuration guides
AO
Ensures new hardware and software products have been approved and documented in the Security Authorization Process documentation
ISSOs
Ensure that adequate security measures are in place to protect access to hardware and software
Ensure that new hardware and software products have been approved in accordance with the configuration management plan prior to installation
Network/ System Administrators
Ensure that hardware and software are properly secured
Ensure that maintenance ports are disabled when not in use
Ensure that unnecessary services are disabled when possible

Hardware and Software Responsibilities
Scan system periodically to identify vulnerabilities and take corrective actions to reduce them
Test software security patches on a non-live system prior to implementation on active production systems
Ensure that new hardware and software products have been approved in accordance with the configuration management plan prior to installation
Facility Managers
Ensure adequate physical security measures are in place to protect access to hardware and software
Ensure that access control policy is enforced
System Owners/Project Managers
Ensure that the installation of hardware and software products meets the configuration requirements specified in applicable DHS secure baseline configuration guides

4.8.5 Personal Use of Government Office Equipment and DHS Systems/Computers

The use of Government-furnished property, including but not limited to office equipment, supplies, computer equipment, software, telecommunications devices, networks, and 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
- Is performed on the employee's non-work time
- Does not reduce productivity or interfere with DHS missions or operations
- Does not violate the *Standards of Ethical Conduct for Employees of the Executive Branch*

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

- Use of Internet sites resulting in an additional charge to the Government
- Obtaining, viewing, or transmitting sexually explicit material or other material inappropriate to the workplace
- Use for other than official Governmental business that results in significant strain on Department 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

A more complete list of inappropriate uses is contained in DHS 4600.1, "Personal Use of Government Office Equipment."

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 DHS SOC provisions of Section 4.9 and of this Handbook's Attachment F, "Incident Response and Reporting."

DHS employees, contractors and others working on behalf of DHS are subject to disciplinary action or sanctions for failure to comply with DHS security policy, regardless of whether or not the failure results in criminal prosecution. Information security-related violations are addressed in "Standards of Ethical Conduct for Employees of the Executive Branch."

Employees can *not* expect privacy when using Government resources. A banner message indicating this policy is required to be displayed on the login screens of DHS computers. This information must also be included in the Rules of Behavior that users are required to sign annually.

Use of Government resources constitutes implied consent to monitoring and auditing of equipment and systems at all times. Monitoring includes tracking of internal DHS network transactions and external transactions such as Internet access. It also includes auditing of stored data on local and network storage devices as well as removable media. DHS is authorized to access email messages or other documents on Government computer systems as part of an investigation or whenever it has a legitimate reason for doing so.

Contractors are not authorized to use Government office equipment or systems for personal use under any circumstances, unless limited personal use is specifically permitted by their contract. When limited use is authorized, contractors are governed by limited personal use policy.

Responsibilities relating to personal use of Government office equipment and DHS systems are provided in the following table.

Personal Use of Government Office Equipment and
Human Capital Office
Establishes DHS policy regarding personal use of Government resources
DHS CIO/CISO
Provides policy and guidance concerning appropriate use of computer resources
Establishes and implements appropriate enforcement policies for noncompliance with computer resource usage policies
Component CISOs/ISSMs
Ensure that controls, including awareness training, are in place to minimize or prevent unauthorized use of Government resources
Supervisors
Enforce personal use policies, including remedial training and other sanctions
Promptly report unauthorized use of Government resources in accordance with DHS incident reporting procedures (see DHS 4300A Attachment F)
ISSOs, Network/System Administrators
Remind users of their system responsibilities and the potential penalties for misuse of system resources
Remind users that they do not have any right to or expectation of privacy while using Government office equipment DHS systems, including Internet and email services

Personal Use of Government Office Equipment and DHS Systems Responsibilities
Users
Become and remain aware of the personal use policies described in this section of the handbook and in other references provided by DHS security officials, including the Standards of Ethical Conduct for Employees of the Executive Branch
Adhere to personal use policies established in this section and in other references provided by DHS security officials
Promptly report unauthorized use of Government resources in accordance with DHS incident reporting procedures (see Attachment F to this Handbook.)
Be aware of and understand the disciplinary actions associated with violations of information security policy, including the unauthorized use of Government resources
Can not have any expectation of privacy in the use of Government computers or computer systems
Contractors and non-DHS Employee Users
Understand and abide by the personal use provisions of the contract or memorandum of agreement with DHS

4.8.6 Wireless Settings for Peripheral Equipment

Peripheral equipment (printers, scanners, fax machines) often includes capabilities, intended to allow wireless access to these devices. Although convenient, wireless access comes with additional risks. In general, wireless access is not allowed on DHS networks.

4.9 Department Information Security Operations

The DHS Security Operations Center (SOC) is the central coordinating and reporting authority for all Sensitive and National Security computer security incidents throughout the Department. The Homeland Secure Data Network (HSDN) Security Operations Center (SOC) reports incidents to the DHS SOC through appropriate channels to protect data classification. The HSDN SOC is subordinate to the DHS SOC, acting as the central coordinating and reporting authority for all SECRET computer security incidents throughout the Department.

Attacks against automated systems continue to increase dramatically. As reliance on computer resources has increased, the systems themselves have become more vulnerable to attack, viruses, system failure, and user error. Attacks have been launched against many organizations and have occurred regardless of the sensitivity and criticality of the data being processed.

Incidents can be accidental or malicious, and they can be caused by outside intruders or internal personnel, causing significant disruption of mission critical business processes and computer-supported operations; these incidents can severely disrupt computer-supported operations, compromise the confidentiality of sensitive information; and diminish the integrity of critical data.

The effects of security incidents can range from embarrassment to interruption of service to inability to function, and, potentially, to loss of human life. A significant concern is that hostile individuals or foreign states could severely damage or disrupt critical operations, resulting in

harm to the public welfare. DHS maintains a security incident reporting and handling capability to help combat the disruptive short and long-term effects of security incidents.

OMB M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," requires that agencies report *all* incidents involving Personally Identifiable Information (PII) to the United States Computer Emergency Readiness Team (US-CERT) within one (1) hour of discovery of the incident. All incidents involving PII in electronic or physical form are to be reported, and no distinction is to be made between suspected and confirmed incidents.

Security incident response and reporting responsibilities are provided in the following table.

Security Incident Response and Reporting Responsibilities
DHS CIO
Determines whether or not security incident information is releasable to the public
DHS CISO
Manages the DHS SOC and the incident reporting program
Advises the DHS CIO on status of significant incident activity
Advises the DHS CIO on the outcome of incident investigations
Distributes incident reports to each Component
DHS SOC
Serves as the focal point for all DHS incident response activities, to include reporting, incident response, and remediation
Component CISO/ISSM
Ensures compliance with DHS incident reporting and violation handling policies
ISSOs
Ensure that system development and site personnel submit incident reports as specified in this section of the handbook
Ensure that system development personnel and system users are trained in the proper procedures for recognizing and reporting security incidents in accordance with the requirements in Attachment F to this Handbook, "Incident Response and Reporting"
System/LAN Administrators
Promptly report computer security incidents in accordance with DHS incident reporting procedures (see Attachment F to this Handbook)
Users
Promptly report information security incidents in accordance with DHS incident reporting procedures (see Attachment F to this Handbook)

4.9.1 Security Incidents and Incident Response and Reporting

The HSDN SOC operates as a separate component, though subordinate to the DHS SOC, in a similar manner to the Component SOCs.

4.9.1.1 DHS SOC Organization

The DHS SOC reports to the DHS CIO; the DHS CIO and DHS CISO provide senior management guidance and direction to the DHS SOC. The DHS SOC provides guidance to Component SOCs.

4.9.1.2 Logging and Monitoring

The DHS SOC maintains visibility into security operations by using logging and monitoring. The DHS SOC 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 element asset integration, requisite event visibility, retention, storage considerations and direction for elements to provide logging events into the DHS SOC toolset and relevant security policy reference.

Department logging guidance is documented in the DHS Logging Strategy in the Department of Homeland Security (DHS) Security CONOPS.

4.9.1.3 Authority and Management

Security operations oversight and management is inherently a Governmental responsibility, not one that can be outsourced solely to contractors. While a Component 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 in response 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 TS/SCI. Ideally all Watch Officers will be TS/SCI cleared. Such clearance is necessary to receive threat intelligence updates at Top Secret (TS) and above.

Because cyber operations are a continuous activity, Government authority must be continuously available. This is commonly is handled by three or more Watch Officers on an eight (8) hour shift rotation, or by Government authority passed from one SOC to another to cover their watch area during off-hour operations. A DHS Watch Area must never be without Government oversight.

4.9.1.4 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."[7] 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

[7] *IT Security Architecture Guidance Volume 2*

vectors and methods of intrusion, thus suggesting measures which can be taken to protect against future incidents.

The DHS SOC, in cooperation with involved Components, will conduct forensic examinations as deemed necessary in accordance with the incident response guidelines detailed in "Incident Response," Attachment F to this Handbook.

In response to an incident requiring computer forensics, the DHS SOC will coordinate support from Components that have appropriate capabilities.

Any investigation that reveals potential criminal activity must be turned over to the appropriate authority. Forensic investigations will normally consist of three tiers, as shown in Table 2, Forensic Investigations Tiers.

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

Table 2 – Forensic Investigations Tiers

4.9.1.5 Vulnerability Management

Vulnerability management is a combination of detection, assessment, and mitigation of systematic weaknesses. Vulnerabilities may be revealed by 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 and Security Control Assessment).

The DHS SOC 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. Such a strategy accounts for vulnerability severity, threats, and assets at risk.

Risk calculation allows Components to prioritize remediation actions, in accordance with specific situations and risk management strategies. Remediation actions are captured in each Component's patch management policy.

4.9.1.6 Information Security Vulnerability Management

The DHS SOC will stay abreast of current system vulnerabilities and provide recommendations to Components through ISVM messages. The DHS SOC will forward advisories from US-CERT, as appropriate, and ensure that each Component is alerted. In cases where the alert, advisory or warning is time-critical, the DHS SOC may also inform each DHS Component CIO and point of contact (POC) via telephone. The Component POCs will be asked to reply to the DHS SOC within a specified time period in instances requiring response to external organizations.

ISVM messages to Components can be of three forms:

- Information Security Vulnerability Alert (ISVA)
- Information Security Vulnerability Bulletin (ISVB)
- Technical Advisory (TA)

The kinds of vulnerabilities, messages, and required Component actions are outlined in Table 3, ISVM Requirements.

	ISVA	ISVB	TA
Risk	Severe	Medium	Low
Acknowledgement	Yes	Yes	No
Compliance*	Yes	Yes	Yes
Compliance Confirmation	Yes	Yes	No
* Compliance is required if affected systems are present within the Component			

Table 3 – ISVM Requirements

Anyone within DHS may be added to the ISVM distribution list. Those wishing to be added must obtain management approval and provide a DHS email address. ISVMs contain sensitive, "For Official Use Only," information and must not be forwarded to non-DHS email accounts.

Although ISVM messages can be sent to anyone, *only Component CISOs/ISSMs* or their designated representatives may acknowledge receipt of messages, report compliance with requirements or send notification of granted waivers.

ISVM messages will have the same general format and will contain the following sections, as applicable:

- Message number
- Version

- Related Common Vulnerabilities and Exposures (CVE) numbers
- Release date
- Subject
- Executive summary
- Requirements
    - Acknowledgment (yes/no)
    - Acknowledge by date
    - Compliance (yes/no)
    - Compliance by Date
    - Reporting Instructions
- Affected systems
- Details
- References
- Required actions
- Recommended actions
- Contact information
- Revision information

See Appendix 6 to the *DHS Security Operations Concept of Operations* for the ISVM Message Template.

Correspondence regarding ISVM notices should be sent via email to dhs.soc@dhs.gov.

4.9.2 Law Enforcement Incident Response

The DHS SOC notifies the DHS Chief, Internal Security and Investigations Division, Office of the Chief Security Officer (CISID-OIS) whenever an incident requires law enforcement involvement. Law enforcement coordinates with the DHS SOC, the CISID-OIS, the Component, and other appropriate parties whenever a crime is committed or suspected.

4.9.3 Definitions and Incident Categories

A security event is a notable but unassessed occurrence that may affect a computing or telecommunications system or network. Security events may result from intentional or unintentional actions and may include inappropriate use of DHS information resources. An event can become an incident after it has been assessed. The assessment process may be performed by the DHS Help Desk, a Component SOC, or the DHS SOC, depending upon its nature and the circumstances. Events are investigated individually, but the Help Desk and SOCs also review them globally for patterns and tendencies that could identify system vulnerabilities.

An information security incident is an assessed security event. It may even be a simple, inadvertent situation that can be rectified by employee training. Security incidents include the inappropriate use of DHS computer resources. Examples include:

- Use of Internet sites that result in an additional charge to the Government
- Obtaining, viewing, or transmitting sexually explicit material or other material inappropriate to the workplace, which might be considered to contribute to a hostile work environment for some employees
- Use for other than official Governmental business that results in significant strain on Department 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

Sometimes, the security incident is a clear violation of an explicit or implied security policy that applies to a computing or telecommunications system or network. DHS has identified several categories of computer security incident and defined them in Attachment F to this Handbook. Examples include:

- Unauthorized attempts to gain access to information
- Introduction of malicious code or viruses into an information system
- Loss or theft of computer media

Categories of incidents include the following:

- Unauthorized Access (Intrusion): Unauthorized access includes all successful unauthorized accesses and suspicious unsuccessful attempts
- Denial of Service: Denial of service attacks include incidents that affect the availability of critical resources such as email servers, Web servers, routers, gateways, or communications infrastructure
- Malicious Logic: Malicious logic includes active code such as viruses, Trojan horses, worms, and scripts used by crackers/hackers to gain privileges and/or information, capture passwords, or modify audit logs to hide unauthorized activity
- Misuse: Misuse occurs when a user violates Federal laws or regulations and/or Department policies regarding proper use of computer resources; installs unauthorized or unlicensed software; or accesses resources or privileges that are greater than those assigned
- PII incident: PII incidents are suspected or confirmed breaches of personally identifiable information in electronic or physical form and are categorized by the manner in which the PII incident occurred (e.g., Alteration/Compromise of Information, Unauthorized Access (Intrusion), Misuse). The DHS SOC Online Reporting System has specific questions that relate to PII incidents, which should be completed in their entirety.
- Probes and Reconnaissance Scans: These include probing or scanning networks for critical services or security weaknesses; This category also includes nuisance scans
- Classified System Incident: Any incident that involves a system used to process national security information

- Alteration/Compromise of Information: Any incident that involves the unauthorized altering of information, or any incident that involves the compromise of information

4.10 Documentation

Documentation of information systems involves collection of detailed information in areas including functionality, system mission, unique personnel requirements, types of data processed, architecture, system interfaces, system boundaries, hardware and software elements, system and network diagrams, cost of assets, system communications and facilities, and any additional system-specific information. This information represents the foundation of the system's configuration baseline. All proposed changes to the configuration baseline must be analyzed and tested to determine whether or not they have any security implications. All proposed configuration changes to operating systems must be analyzed, as must operating system security features, applications, critical system files, and system devices. Changes must be approved through a formal Change Control Board (CCB) and must be fully documented before they are implemented. Change control policies must consider and have provisions for quickly testing and approving time-sensitive changes that result from newly available vulnerability information.

The software, firmware, algorithms, data structures, processes, and other design mechanisms that satisfy a set of documented security requirements make up the system's security baseline. Security elements of operational systems should be set to their most restrictive mode prior to placing the system into the operational environment.

Adequate records of changes to the configuration or security baseline must be maintained for each system. A historical log of changes for all previous configurations must be maintained. Periodic configuration reviews are conducted in conjunction with periodic risk assessments.

Documentation responsibilities are provided in the following table.

Documentation Responsibilities
Component CISOs/ISSMs
Ensure that security issues are formally documented and tracked during the SELC process
Project Managers/ISSOs
Ensure that change control procedures are documented and implemented for all proposed configuration changes to systems
Ensure that all proposed configuration changes to operating systems, operating system security features, applications, critical system files, and system devices are formally approved and documented prior to the change being implemented
Maintain a capability to quickly approve and implement time-sensitive security patches in reaction to late-breaking notification of security vulnerabilities identified by the DHS SOC
Ensure that all approved changes to the configuration baseline are documented and reviewed for accuracy, and that records are maintained for each system for both current and all previous configurations
Ensure that formal system configuration reviews are performed
Ensure that accurate system documentation and configuration logs are maintained to reflect current and

Documentation Responsibilities
prior configuration baselines

4.11 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 interruption of service. A Backup Operations Plan must be included in the Contingency Plan, as discussed in Section 3.5.2, "Information Technology Contingency Planning."

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 Contingency Plan) 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 in the following table.

Information and Data Backup Responsibilities
Component CISOs/ISSMs
Establish and enforce backup policy
Provide technical expertise and evaluate the effectiveness of backup approaches
Security Control Assessors
Ensure that a Backup Operations Plan is included in the Contingency Plan
System Owners
Ensure that a backup strategy and procedures are established, implemented, and tested in accordance with the Contingency Plan
System/Network Administrators
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

Information and Data Backup Responsibilities
Ensure that at least one backup copy of system software is retained off-site
ISSOs
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 responsibility to back up any sensitive data residing on their hard drives
Review the Contingency Plan as part of the 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
Users
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

4.12 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 data and may also be connected to data communications networks.

The use of nontraditional information systems elements without appropriate safeguards presents risks to DHS organizations in part because these devices are typically not thought of as information systems.

Wireless devices must be secured as specified in Section 4.6, Wireless Communications. Copiers with the capability to process sensitive documents must be secured in the same manner as facsimile machines (see Section 4.5.2). Sanitization of media included in copiers (or other devices) must be carried out in the manner prescribed in Section 4.3.3, Media Sanitization and Disposal. If the device is a multifunction device, the fax functions must be secured in the same

manner as stand-alone fax machines. Printing functions must be secured in accordance with the provisions of Section 4.3.4, Production, Input/Output Controls.

HVAC, fire suppression, and power equipment (including emergency power backup) must be secured in accordance with the requirements specified for PBXs, as described in Section 4.4.1. 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 DHS networks, must be clearly documented in the Security Plan and authorized for that functionality. The risks of using such devices must be identified along with countermeasures employed to mitigate these risks. This information must be included in applicable Rules of Behavior and addressed in awareness training orientation and refresher sessions.

Responsibilities related to converging technologies are provided in the following table.

Converging Technologies Responsibilities
ISSOs
Ensure that nontraditional information system elements connected to sensitive systems meet the security requirements detailed in this handbook and are assessed and authorized for that purpose
Ensure media storage devices included in copiers, fax machines, printers, etc., are properly sanitized before leaving DHS control
Ensure audit logs are maintained and reviewed for nontraditional information system elements that store or process sensitive information
Network/System Administrators
Protect and monitor network connections to nontraditional information system devices such as fax 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 CONTROLS

The design of information systems that process, store, or transmit sensitive information is required to include the automated security features discussed in this section. Security safeguards must be in place to ensure that each person having access to sensitive information systems is individually accountable for his or her actions while utilizing the system.

Technical controls are 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.

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 ID.

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)

DHS systems must be designed to ensure that each user is authenticated prior to being allowed access. 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 AO.

Identification and authentication responsibilities are provided in the following table below.

Identification and Authentication Responsibilities
DHS CISO
Establishes and enforces identification and authentication policy
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 system access.
System Owners/Project Managers
Ensure that adequate resources are budgeted for information assurance; assess identification and authentication technology opportunities for potential application to DHS systems

Identification and Authentication Responsibilities
System/Network Administrators
Ensure that the system identifies every user as unique
Secure and administer privileged accounts using authentication technology stronger than passwords
ISSOs
Brief users on identification and authentication procedures and protection requirements
Monitor and enforce compliance with identification and authentication requirements
Perform system audits to verify compliance
Users
Comply with identification and authentication guidance, specifically guidance pertaining to password management (see Section 5.1.1.1)
Report violators of security policies

5.1.1 Passwords

The least expensive method for authenticating users is a password system in which authentication is performed each time a password is used. More sophisticated authentication techniques, such as Smart Cards and biological recognition systems (e.g., retina scanner, handprint, voice recognition), must be cost-justified through the risk assessment process.

A password is a sequence of characters used for authentication purposes. Passwords are often used to authenticate the identity of a system user and, in some instances, to grant or deny access to private or shared data.

Passwords provide a reasonable degree of authentication and are one of the most common methods used for controlling system access. Passwords are important because they are often the first line of defense against intruders or insiders who may be trying to obtain unauthorized access to a DHS system. To be used effectively, policies requiring strong passwords must be implemented, and users and system administrators must follow DHS password guidelines.

The use of a personal password by more than one individual is prohibited throughout DHS. It is recognized, however, that, in certain circumstances such as the operation of crisis management or operations centers, watch team and other duty personnel may require the use of group User IDs and passwords.

5.1.1.1 Selecting Strong Passwords

DHS Sensitive Systems Policy Directive 4300A makes the use of strong passwords mandatory, and requires ISSOs to determine and enforce measures to ensure that strong passwords are used. Therefore, users must select well-constructed passwords. The following table contains guidelines based on DHS policy and "US Government Configuration Baseline" (USGCB) *http://usgcb.nist.gov/* for strong passwords that should be followed throughout the Department:

Required Action	Benefit Gained
Strong passwords : Are at least 12 characters in length. Comply with the DHS hardening guides for operating systems and the configuration guides for applications. In the absence of guidance, the ISSO will determine the appropriate password complexity based on the level of risk. Are not the same as any of the user's previous 8 passwords.	These requirements make it more difficult for a password guesser to obtain passwords. They increase the set of combinations that must be guessed and provide a mixture to defeat a dictionary attack.
Strong passwords do not contain any dictionary word.	Prevents dictionary type of attacks.
Strong passwords do not contain any proper noun or the name of any person, pet, child, or fictional character. Passwords do not contain any employee serial number, Social Security number, birth date, phone number, or any information that could be readily guessed about the creator of the password.	Helps prevent a password guess based on a hacker's personal knowledge of the user.
Strong passwords do not contain any simple pattern of letters or numbers, such as "qwerty" or "xyz123".	Protects against dictionary attacks
Strong passwords do not contain any word, noun, or name spelled backwards or with a single digit appended, or with a two-digit "year" string, such as 98xyz123.	Protects against dictionary attacks
Strong pass phrases, if used in addition to or instead of passwords, follow the same guidelines.	Consistent application of guidelines.
Strong passwords are not the same as the User ID.	Risk of unauthorized access is reduced, as hackers initially try "obvious" passwords such as username and User ID.

5.1.1.2 Results of Weak Passwords

Hackers have access to a variety of password-cracking tools. Weak passwords may allow internal or external users or hackers to gain unauthorized access to DHS systems.

Brute force attacks involve manual or automated attempts to guess valid passwords. There are numerous password-guessing programs available on the Internet. Most hackers have a "password hit list," which is a collection of default passwords automatically assigned to various system accounts. For example, the default password for the guest account in most UNIX systems is "guest."

Many hackers will try to guess passwords using a user's personal information, such as birth date, name of spouse or children, pets, employee ID number, etc. Hackers will often practice what they call "social engineering," which involves talking with employees to find out things about

the systems in their office, and, more importantly, personal information that will help them guess passwords.

Users tend to choose passwords that are easy to remember such as the name of a family member or pet, a birth date, or a word that may mean something to the user. These types of passwords are the easiest for others to guess.

People are the key to constructing good passwords. Poorly constructed passwords make it easier for a hacker to crack the password. The longer it takes hackers to get a password, the more likely they are to move on to other methods of gaining access to the system.

It should be noted that many computer systems use auditing features that keep a record of actions initiated by the users while on the system. Once a hacker cracks a password and gains access to the system using the appropriate User ID, the system audit logs record that the User ID was used in taking harmful actions on the system. Authentication is the basis for control and accountability of the users on the system.

5.1.1.3 System Administrator Responsibilities

System administrators should follow the DHS password guidelines in the following table to ensure that password settings are in compliance with DHS requirements.

A secure method for distribution of passwords is also necessary. Administrators must verify an individual's identity prior to communicating account or password information.

Recommended Action	Benefit Gained
Do not store passwords in a clear text file.	Avoids situation where convenience and speedy login are achieved at the expense of security.
Passwords are to be changed or expire in 90 days or less.	By increasing password variability, reduces the likelihood of unauthorized penetrations
Do not enable a password to be reused for at least 8 iterations.	By increasing password variability, reduces the likelihood of unauthorized penetrations
Allow only one user per account; never share User IDs or passwords.	Provides user accountability.
Never assign a login account a password that is the same string as the User ID or that contains the User ID.	Eliminates the hackers' first line of attack, which is to try User ID as the password once they get a telnet prompt.
Never install a guest/guest account.	Prevents penetration via certain well-known vulnerabilities in some User Datagram Protocol User Datagram Protocol (UDP) services.

Recommended Action	Benefit Gained
Deactivate unused accounts monthly. For systems with a low impact for the confidentiality security objective, consider an account unused if no login has occurred in 90 days. For systems with a moderate or high impact for the confidentiality security objective, consider an account unused if no login has occurred in 45 days.	Prevents a formerly authorized user from continuing to use the host.
No accounts will be named anonymous, ftp, telnet, www, host, user, bin, nobody, etc.	Avoids accounts commonly attacked via the password-guessing method: e.g., ftp/ftp.
The manager or owner of the host will revalidate the list of User IDs at least annually.	Best security practice to clean out User IDs of ex-employees and to verify which User IDs are valid.
Never set any password equal to the null string, which is equivalent to no password at all.	Follows best security practices.

Privileged accounts must be secured by authentication technology stronger than that based only on a User ID and password. All actions taken by remote privileged users must also be logged for auditing purposes and must be encrypted to prevent "playback" attacks. All passwords, algorithms, keys, certificates, codes, or other schemes used for authentication must be stored in a manner that prevents unauthorized access.

5.2 Access Control

Access controls restrict access to objects such as files, directories, and devices based upon users' identities or groups and protect against unauthorized disclosure, modification, or destruction of the data.

Automated systems are vulnerable to the fraudulent or malicious activities of 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's engaging in fraudulent or malicious behavior while acting alone. The Principle of Least Privilege states that users should only be able to access the system resources needed to fulfill their job responsibilities. This principle should be considered when granting access.

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.*

Network and system administrators 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 element devices, dial-up connections, and network addresses and protocols, or to remove or alter programs be tightly controlled, with access limited to a select group of authorized personnel.

- **Initial User Access**

  Users who need access to DHS systems and networks must have completed a background investigation prior to being granted access. User access will vary depending on the user's position. The user's supervisor or Project Manager must also determine the systems the user needs to access and the levels of access the user requires. The System Owner must approve user access privileges.

- **Review of Access Privileges**

  The data a user needs to access will change over time. Therefore, supervisors have the responsibility to ensure that access control lists are current and 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 process and during annual self-assessments.

  Access control policies and procedures are written and stored in an off-site location. They must 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 and local area network (LAN) administrators and ISSOs must ensure that all departing employees have their access privileges terminated immediately. No former employee should have the ability to access system resources after their term of employment has ended. Procedures vary depending on whether the separation is voluntary of involuntary. Termination of access privileges also applies to employees whose job functions have changed such that they no longer require access to the level to which they were previously granted. See Section 4.1.6, Separation from Duty, for additional guidance.

- **Secure Remote Access**

  Hardware security tokens, such as cryptographic smartcards, can be issued to DHS employees and contractors who have a valid need to remotely access DHS systems and data.

Users are responsible for protecting all DHS information to which they have access.

Access control responsibilities are provided in the following table.

Access Control Responsibilities
Component CISOs/ISSMs
Establish and enforce access control policy
Provide technical expertise and evaluate the effectiveness of access control approaches
Security Control Assessors
Conduct assessments to verify that adequate access controls are in place

Access Control Responsibilities
System/Network Administrators
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 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

Components must configure each information system to lock a user's account for a specified period following a specified number of consecutive failed logon attempts. Users must be locked from their account for a period of twenty (20) minutes after three consecutive failed logon attempts. All failed logon attempts must be recorded in an audit log and periodically reviewed.

Automatic account lockout responsibilities are provided in the following table.

Automatic Account Lockout Responsibilities
DHS CISO
Establishes and enforces automatic account lockout policies
System/Network Administrators
Ensure that systems are configured to lock a user's account for 20 minutes after 3 unsuccessful logon attempts during a 24 hour time period
ISSOs
Ensure that systems are configured to lock a user's account for 20 minutes after 3 unsuccessful logon attempts

5.2.2 Automatic Session Termination

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

Automatic session lockout responsibilities are provided in the following table.

Automatic Session Lockout Responsibilities
DHS CISO

Automatic Session Lockout Responsibilities
Establishes and enforces automatic session lockout policies **System/Network Administrators** Ensure that systems are configured to terminate any user session that has remained idle for 20 minutes **ISSOs** Ensure that systems are configured to terminate any user session that has remained idle for 20 minutes

5.2.3 Warning Banner

The DHS CISO stipulates that a warning banner statement be displayed on all DHS systems during logon. The most current language can be found on the DHS CISO Web page.

Please note that the current warning banner was developed specifically for use on DHS workstations. Due to differing function, purpose and situation as well as 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.

Warning banner responsibilities are provided in the following table.

Warning Banner Responsibilities
DHS CISO Establishes and enforces the use of appropriate standard Warning Banner for all DHS systems **System/Network Administrators** Ensure that DHS systems under their control are configured to display the approved DHS Warning Banner **ISSOs** Ensure that all DHS systems under their control are configured to display the approved DHS Warning Banner

5.3 Auditing

Auditing is a fundamental security principle that provides the ability to track the activities of a user who is accessing an automated system. Trails maintained by auditing tools are an effective method of enforcing this principle. Audit trails maintain a record of system, application, and user activity.

With the use of appropriate tools and procedures, auditing can further progress toward several security-related objectives including:

- Individual accountability

- Intrusion detection
- Problem identification
- Capability to reconstruct events

Audit trails can track the identity of each subject attempting to access a system, the time and date of access, and the time of log off. Audit trails can also 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 to allow rapid access to recent information. Audit trails should be preserved for a period of seven years as part of record management 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 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 capability 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 need to be secured to prevent tampering and they must be backed up regularly.

Auditing responsibilities are provided in the following table.

Auditing Responsibilities
Component CISOs/ISSMs
Ensure that all DHS systems maintain audit records sufficient to reconstruct security related events
Evaluate auditing requirements at the Component level
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 managers to identify critical functions to be subjected to auditing and keep apprised of audit findings.
Ensure auditing is performed independently of system/network administration
System/Network Administrators
Maintain an audit record sufficient to reconstruct security related events
Ensure that each audit record includes:

Auditing Responsibilities
– The identity of each person and device accessing or attempting to access the system.
– The time and date of the access or attempt and when the user logged off
– Activities performed using an administrator's identification
– Activities that could modify, bypass, or negate the system security
– Sufficient detail to facilitate reconstruction if compromise or malfunction occurs
– Security related actions associated with processing
Protect audit records against unauthorized access, modification, or destruction
Retain audit records for a minimum of ninety (90) days or in accordance with the Security Plan 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 DHS system that does not implement an auditing capability
Ensure that audit records include all required elements
Review audit records at least weekly, or in accordance with the SP
Ensure that audit collection and review procedures contain provisions for adequate separation of duties Report security related events to the Component's Security Operations Center (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.

5.4.1 Remote Access and Dial-In

Remote access technology allows trusted employees to access DHS networks by dialing in via modem or accessing the DHS network via the Internet. This allows mobile employees to stay in touch with the home office while traveling. There are significant security risks, however, 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.

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

Remote access solutions that do not comply with the requirements of FIPS 140-2 are not authorized.

Remote access and dial-in responsibilities are provided in the following table.

Remote Access and Dial-In Responsibilities
Component CISOs/ISSMs
Establish and enforce the remote access control policy for each Component
Provide technical expertise and evaluate the effectiveness of remote access control approaches
System/Network Administrators
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

5.4.2 Network Security Monitoring

Security monitoring, detection, and analysis are key functions and are critical to maintaining the security of DHS 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.

Component SOCs lead the network security monitoring effort. Component CISOs/ISSMs, ISSOs, and system/network administrators 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.

Network security monitoring responsibilities are provided in the following table.

Network Security Monitoring Responsibilities
Component CISOs/ISSMs
Establish Component policy and implement and manage a viable intrusion detection program within their Component
Provide guidance, as needed, when responding to intrusion alerts from the DHS or Component SOC
DHS and Component SOC

Network Security Monitoring Responsibilities
Monitor DHS 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 SOCs
Participate in SOC-led incident response investigations
Evaluate the impact of the event on the system
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 block every avenue to 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. Intrusion detection systems 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 statistically established 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 Monitoring

The DHS SOC is responsible for monitoring of DHS systems and networks. Upon receipt of an alarm, operators investigate to determine the validity of the alarm. Once validity is confirmed, the operator notifies the ISSO and/or the system administrator for corrective action. If the problem is deemed critical, senior management is notified and must be involved in determining 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 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.

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 and systems to ascertain whether or not changes have occurred that could adversely affect security.

Network connectivity responsibilities are provided in the following table.

Network Connectivity Responsibilities
Component CISOs/ISSMs 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** 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 **Network Administrators** Ensure technical controls governing use of the external connection remain in place and function properly Assist in development of the ISA **ISSOs** Coordinate with the external agency in development of the ISA Assist in preparation of the ISA and ensure all external connections are documented in the SP, Risk Assessment, and security operating procedures Review ISAs as a part of the annual FISMA self-assessment Monitor compliance **Users** When connecting to DHS networks, ensure the equipment used to access the 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 National Institute of Standards and Technology (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 or AO. The ISA documents the security protections on the interconnected systems to ensure that only acceptable transactions are permitted. Component personnel must review ISAs as part of the annual FISMA self-

assessment. ISAs must be reissued every three (3) years or whenever significant changes have been made to any of the interconnected systems.

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

An ISA should contain the following:

- 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.
- Interconnection Statement of Requirements – This section documents the formal requirement for connecting the two systems. The following items should be addressed in this section:
    - The names of the systems being interconnected
    - The requirement for the interconnection, including the benefits derived
    - The type of connection (Frame Relay, T1, etc.)
    - Physical location of connection equipment, including addresses and room numbers
    - Primary Points of Contact (POC) for both systems
    - The agency name(s) or organization that initiated the requirement.
- 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 aspects 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 should be included.
- 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:
    * All data communications paths (not program system paths), circuits, etc., used for the interconnection beginning with the DHS-owned system(s) and including all interconnected systems to the non-DHS end-point
    * The logical location of all elements (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).
- Signatures and Comments – Each ISA must be signed by the AO of each interconnecting system 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 by the AOs of the interconnected systems. Others in the organization, however, should have the opportunity to review changes.

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

5.4.3.2 Trust Zones

Information and services sharing between the DHS SOC and Components 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 SOC must be aware of Component-security requirements, as defined by Trust Zones, to accurately perform DHS SOC duties.

DHS Trust Zones have the following characteristics:

- The Trust Zone must be set of networked hosts protected from unconstrained access by one or more security perimeter devices
- There must be a basis for placement and configuration of firewalls, Virtual VPNs, and remote access protection devices
- The Trust Zone may consist of a single host, one or more LANs at a site, or a group of networks connected via a network provider or backbone
- OneNet provides a layer of trust by means of sub-netting, firewalls, and other policy enforcement mechanisms
- 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

5.4.4 Firewalls and Policy Enforcement Points

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

Within DHS, boundary protection of information system 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, data encryption, personnel background checks, security guards, , and physical security barriers, provide an added level of assurance that unauthorized personnel will be unable to access the Department'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.

Responsibility for deployment and management of firewalls are included in the following table.

Firewall Responsibilities
Component CISOs/ISSMs
Develop procedures and schedules for deploying firewall systems
ISSOs and ADP Support Personnel
Assist Component teams in the installation and configuration of firewall systems
Site Managers
Ensure that the firewall installation team receives necessary support during and after installation
SOCs
Manage firewalls in accordance with DHS firewall policy
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 vary widely. 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. 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, personal digital assistant (PDA), mobile phone, 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 two-factor authentication mechanism, and 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 the firewall. Encryption, moreover, involves use of 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.

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 DHS 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, the Department 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 sensitive systems must be under the control of DHS and Component SOCs, who are responsible for providing direction and guidance for firewall settings and rule sets. The actual application of all firewalls is under the DHS SOC.

5.4.5 Internet Security

Section 5.4.5 of DHS Sensitive Systems Policy Directive 4300A provides specific DHS technical policy regarding the use and proper configuration of firewalls and the management of dial-up connections and other protocols.

Sound network security practice dictates that all network connections be identified and that the threats and vulnerabilities associated with these connections be analyzed. The guidance provided in Section 5.4.3, *Network Connectivity*, specifically that with regard to ISAs, and in Attachment N to this Handbook, "Interconnection Security Agreements," also applies to connections to the Internet and extranets. 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 entities, which may include suppliers, vendors, and customers. An extranet requires security and privacy and may involve firewalls, digital certificates, message encryption, and virtual private networks 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 Process 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 Component personnel and documented in the annual information security assessment.

Adequate protection requires proper selection and installation of firewalls and other boundary devices, Intrusion Detection Systems, and ancillary encryption or filtering devices. These devices must be assessed and authorized prior to their use on DHS networks. Implementation guidance for firewalls is discussed in Section 5.4.4 of this Handbook, "Firewalls." Intrusion Detection Systems are covered in Section 5.4.2; encryption is addressed in Section 5.5.1. The

adequacy of all of these must be monitored and reviewed as part of periodic information security assessments.

Firewalls must be configured so as 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 Server Message Block (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 DHS 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" (unencrypted human-readable text), which allows Internet service providers (ISPs) and other users on the Internet, intranet, or LAN to intercept and read the traffic. Telnet use 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 Secure Shell (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 (ISPs) 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) element of SSH. SSH is a 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 must be used only in conjunction with appropriate countermeasures and risk-reduction procedures:

- Cross boundary routing broadcasts
- 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. Dial-in connections, to the extent they can even be justified, must be strictly controlled.

Internet security responsibilities are provided in the following table.

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

5.4.6 Email Security

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

DHS SOC personnel are trained to respond to incidents pertaining to email security and

assist the email gateway Steward as necessary. Components must provide appropriate security for their email systems.

Email is the most commonly used application for exchanging data electronically. The email process is divided into two main elements:

- Mail servers, which deliver, forward, and store mail
- 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 capabilities similar to email, but are inherently less secure; the technology to secure. 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 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 Instant Messaging 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:

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

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

Components 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 nonrepudiation 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. Network design alone, however, cannot protect a mail server. The following steps need to be accomplished on a according to a regular schedule:

- Review and analyze log files
- Back up data daily (or in accordance with the SP)
- 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.

Note: Due to the significant risk associated with HTML email, DHS is considering following the lead of the Department of Defense (DOD) and moving to text based email.

Email security responsibilities are provided in the following table.

Email Responsibilities
DHS CISO
Establishes Department-wide policy to secure email systems
Component CISOs/ISSMs
Advise the DHS CISO on methods for securing Department email systems
Enforce Department email security policies
Security Control Assessors
Conduct assessments to determine that adequate security controls are in place for email systems
AOs
Ensure that adequate email security controls are in place prior to authorization of the system
System/Network Administrators
Ensure that email security controls are in place and functioning as intended
Ensure that email security controls provide the security features named in this document
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 log files.
Back up data as required by the Security Plan
Protect email systems against malicious code
Deploy the following network protection mechanisms: – Firewalls – Routers – Switches – Intrusion detection systems
ISSOs
Schedule semiannual or quarterly appointments with the SOC or 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 named in this document and in the SP
Ensure that a tested Contingency Plan is in place

5.4.7 Personal Email Accounts

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

Sending email to a personal account has the following vulnerabilities:

- DHS does not authorize the use of personally owned computers within DHS; they are not likely to have the appropriate encryption software installed, thus information is sent in "clear text"
- The route that the email travels cannot be predicted
- Untrusted persons at ISP sites may read sensitive information
- Email travels over unprotected communication links that can be "sniffed" in transit, exposing messages to being read by unauthorized persons
- Web browsers are often used to access private email accounts and such access is inherently not secure
- Malware (which could exist on the employee's personal computer) can send copies of existing emails or other text on a victim's computer to unknown individuals
- Instant Messaging channels are a frequent source of malware and of mechanisms for attacks on personal computers
- So-called "spyware" programs transmit information from personal computers to unknown sites. Some 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.

Personal email responsibilities are provided in the following table.

Personal Email Responsibilities
DHS CISO
Establishes DHS policy concerning the transmittal of sensitive information
Evaluates the risks associated with the transmittal of sensitive information
Component CISOs/ISSMs
Evaluate the risks and recommend solutions to counter the risk of transmitting sensitive information
System Owners and Supervisors
Enforce DHS policy prohibiting the transmittal of sensitive information to personal email accounts
System Administrators
Ensure that technical controls are in place and properly functioning to prohibit and/or deter the

Personal Email Responsibilities
transmission of sensitive DHS information to personal email accounts **ISSOs** Ensure that technical controls are in place and properly functioning to prohibit and/or deter the transmission of sensitive DHS information to personal email accounts Monitor compliance with DHS policy compliance **Users** Comply with DHS policy prohibiting the transmission of sensitive information to personal email accounts

5.4.8 Testing and Vulnerability Management

The DHS SOC takes a proactive approach to vulnerability management including detecting vulnerabilities through testing, reporting through Information System Vulnerability Management (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.

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.

The DHS ISVM Program, managed through the SOC, provides Component CISOs/ISSMs and operational support personnel (e.g., ISSOs, System Administrators) with bulletins, alerts, and technical advisories related to emerging vulnerabilities and threats. The ISVM is modeled on the Department of Defense Information Assurance Vulnerability Assessment (IAVA) program but generally does not prescribe mitigation options nor centrally manage software patching. The following ISVM tools are available to support the Component CISO/ISSM:

- DHS 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 Appendix O2 of DHS 4300A Attachment O to this handbook)
- Negotiated pricing for vulnerability assessment tools (pending)

The DHS Vulnerability Management Program is described in "Vulnerability Management," Attachment O to this Handbook. 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 Process tool with a built-in vulnerability assessment capability. In

addition, Plans of Action & Milestones (POA&M) will be prepared and used in conducting periodic vulnerability testing and assessments of information security controls and techniques.

Testing and vulnerability assessment responsibilities are provided in the following table.

Testing and Vulnerability Assessment Responsibilities
Component CISOs/ISSMs
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 Systems Engineering Life Cycle (SELC) support
Ensure coordination among the DHS SOC, the Component SOC, and the ISVM Program when vulnerability assessments cross multiple Component responsibilities
ISSOs and Information System Support Personnel
Support SOC vulnerability assessments

5.4.8.1 Vulnerability Scanning

Vulnerability scanning is the process of identifying known vulnerabilities of information systems operating on a network in order to determine if a system can be compromised. Vulnerability scanning often employs software that contains databases of known flaws, and tests systems for the occurrence of these flaws.

Vulnerability scanning typically refers to system audits on internal networks that are not connected to the Internet, as well as to systems that are visible on the Internet. The purpose of vulnerability scanning is to identify weaknesses in a system (or in system security procedures, hardware design, internal controls, etc.) that could be exploited to gain unauthorized access or to affect the systems' availability or data integrity.

Staff members performing this type of testing must be cleared to the levels commensurate with that of the system being tested.

5.4.8.2 Expanded Vulnerability Scanning

The type of security testing performed by general-purpose vulnerability scanning tools may uncover weaknesses in the underlying elements of systems that host DHS intranet or Internet web sites. A special class of scanning tools explores weaknesses in elements 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 the website draws data that it displays. A similar class of database vulnerability tools exists for databases. These tools 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 elements. For example, firewalls may provide barriers to standard discovery techniques. Specialized scanning tools, however, can use 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.

5.4.8.3 Gap Analysis

Gap analysis determines the variance between requirements current capabilities. It 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.

5.4.8.4 Penetration Testing

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 Internet Categorization of Attacks Toolkit (ICAT) database can provide a laundry list of possible vulnerabilities in the hardware, operating systems, middleware, or applications discovered.

5.4.8.5 Scope of Vulnerability Assessments

All equipment attached to the DHS information system 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 potential threats to the health of the DHS infrastructure.

Proactive security scanning allows for a meaningful assessment of system security against known risks, provides a roadmap of effective countermeasures for improving security, leads to faster detection of vulnerabilities, and reduces damage to breached systems. Proactive scanning can also identify authorized and unauthorized devices on the internal network, such as

unauthorized wireless access points, modems or high-speed links installed by employees for their personal convenience.

Any system identified in conjunction with a security incident is subject to a comprehensive security scan. Random network scans will not be advertised, but the DHS SOC will be informed prior to conducting any scans.

Network and host scans are to be conducted by authorized DHS 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.

5.4.9 Peer-to-Peer Technology

Peer-to-peer technology refers to applications that allow individual PCs to act as servers to other individual PCs. This technology was made popular by music file-swapping services (e.g., Napster, Kazza, etc.). 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. Each computer has the ability to act as a both a server, by hosting files for others to download, and a client by searching other computers 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.

Peer-to-peer applications circumvent most enterprise security systems. This provides malicious users easy access, allowing them to install malware, identify IP addresses or user names, launch denial of service attacks, gain control of network resources, or access sensitive information.

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.

[For additional information on inappropriate use of DHS resources, see Section 3.12, “Information Technology Security Policy Violation and Disciplinary Action;” Section 4.8.3, “Personally Owned Equipment and Software;” Section 4.8.5, “Personal Use of Government Office Equipment and Department of Homeland Security Information Technology Systems/Computers;” and Section 4.9, “Security Incidents and Incident Response and Reporting.”]

Peer-to-peer responsibilities are provided in the following table.

Peer-to-Peer Technology Responsibilities
DHS CIO, CISO
Establish DHS policy regarding the unauthorized use of information system technology and software
Component CISOs/ISSMs
Ensure that controls, including awareness training, are in place to minimize or prevent unauthorized use of unauthorized information system technology and software
Supervisors
Enforce unauthorized use policies including remedial training and other sanctions
Promptly report unauthorized use of information system technology in accordance with DHS Computer Security Incident reporting policy (see Attachment F to this Handbook)
ISSOs, Network/System Administrators
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 information system technology in accordance with DHS Computer Security Incident reporting policy (Attachment F to this Handbook)
Users
Be aware of the prohibition against the use of unauthorized information system technology and software
Adhere to the Unauthorized Use policies established in this section and in other references provided by DHS security officials
Promptly report unauthorized use of information system technology in accordance with DHS Computer Security Incident reporting policy (Attachment F to this Handbook)
Be aware of and understand the ramifications of penalties involving infractions of the rules regarding inappropriate use of Government resources

5.5 Cryptography

Cryptography is a branch of mathematics that deals with the transformation of data. Cryptographic transformation converts ordinary text (plaintext) into coded form (ciphertext) by encryption; and ciphertext into plaintext by decryption.

This science relies on two basic components, namely an algorithm, for example 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.

The two basic types of cryptography are: secret key systems (also called symmetric key systems) and public key systems (also called asymmetric key 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 publically 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.

5.5.1 Encryption

Encryption is the process of changing plaintext into ciphertext for the purpose of security or privacy.

Encryption responsibilities are provided in the following table

Encryption Responsibilities
DHS CISO Develops DHS cryptography policy and approves Component encryption methodologies **AOs** Ensure that sensitive or classified encryption applications under their authority have developed encryption plans for systems prior to authorization Ensure that personnel implementing encryption requirements are technically qualified and adequately trained in encryption technologies and in the specific methodologies employed **Component CISOs/ISSMs**

Encryption Responsibilities
Ensure that DHS encryption policy is implemented and enforced
Advise Project Managers on the implementation of DHS encryption standards
ISSOs
Ensure that encryption is properly implemented and configured on DHS systems
Assist System Owners in identifying sensitive DHS data that requires encryption

5.5.2 Public Key Infrastructure

A 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).

Specific requirements for PKIs which must be met are detailed in DHS Sensitive Systems Policy Directive 4300A.

PKI responsibilities are provided in the following table.

Public Key Infrastructure Responsibilities
DHS CISO
Provides PKI oversight at the Department level
Serves as the DHS PKI Policy Authority
Appoints a DHS PKI Operational Authority
Creates and maintains a DHS CP that complies with the U.S. Federal CP for the Federal Bridge CA
Establishes and maintains the DHS PKI High Assurance Root Certificate Authority (CA)
Ensures that all DHS CAs are subordinate to the DHS Root CA
Specifies the requirements and process for becoming a subordinate CA
Authorizes subordinate CAs
Ensures the DHS Root CA cross-certifies with the Federal Bridge CA at the High, Medium, and Basic Assurance levels
Ensures that all DHS CAs operate under an approved CPS that complies with the DHS CP
Approves Certification Practices Statements for all DHS CAs
Ensures that all DHS CAs undergo a compliance audit at least annually, and specifies a DHS PKI Auditor to perform the compliance audits
Specifies the DHS PKI Auditor to conduct compliance audits
Ensures that appropriate facilities are available for hosting DHS certificate authorities as appropriate for their level of assurance and associated mission. Ensures that appropriate continuity planning is established for all infrastructure that distributes, houses, or stores public keys
Ensures that a DHS PKI archive facility is established and maintained to store PKI records
Ensures that certificates issued by test, pilot, or other CAs in DHS that are not established as subordinate CAs to the DHS Root CA are not be used to protect sensitive DHS operational data, or for authentication on DHS operational systems containing sensitive data
DHS Office of Security
Ensures that PKI registration activities under its purview are performed in compliance with the applicable CPSs
DHS PKI Operational Authority
Provides oversight of PKI operations at the Department level
Creates and maintains all PKI CPSs pertaining to the DHS PKI
Creates and manages DHS PKI Operating Procedures
Oversees and reviews management of DHS PKI Operations for each authority certified subordinate to the DHS Root CA
Works with DHS and Component physical security entities and/or local registration authorities to oversee the issuance and management of certificates across the DHS enterprise

Public Key Infrastructure Responsibilities
Ensures that all aspects of DHS PKI services, operations and infrastructure related to certificates issued under the DHS CP are in accordance with the requirements, representations, and warranties of the CP
Component CISOs/ISSMs
Ensure that PKI registration activities under their purview are performed in compliance with the applicable CPSs
AOs
Ensure that DHS encryption policy is addressed in the Security Plans for information systems that process sensitive information
ISSOs
Ensure that adequate security measures are in place to protect access to hardware and software
Ensure that new hardware and software has been approved in accordance with the configuration management plan prior to installation
Network/System Administrators
Ensure that DHS cryptographic systems are properly configured and functioning properly

5.5.3 Public Key/Private Key

A public key certificate is used to obtain subscribers' public keys in a trusted manner. Once a certificate is obtained, the public key can be used:

- To encrypt data for that subscriber so that only that subscriber can decrypt it
- To verify that digitally signed data was signed by that subscriber, 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.

Public key/private key responsibilities are provided in the following table.

Public Key/Private Key Responsibilities
DHS CISO
Ensures that the DHS CP and CPSs enforce 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 when use of separate public/private key pairs for encryption and digital signature is supported by the protocols native to the type of device.
Ensures that the DHS CP and CPSs require that a human sponsor represent each organization, application, code-signing, and device subscriber when they apply for one or more certificates from a

Public Key/Private Key Responsibilities
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 DHS CPSs require that a mechanism be provided for each DHS CA to enable PKI registrars to determine the authorized human sponsor for each organization, application, code signer, or device. 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. **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 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

Public Key/Private Key Responsibilities
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. **Component CISOs/ISSMs** 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, which enables 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. 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 that human subscribers are aware of their responsibilities to protect their private keys. Ensure that 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 their signed DHS PKI Subscriber Agreement for Human Users and review it at least annually. **Sponsors** Assume responsibility security of the private keys of the subscribers that they sponsor. Abide by their signed DHS PKI Subscriber Agreement for Sponsors and review it at least annually.

5.6 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.

5.6.1 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 – 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 an 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 covertly. A Trojan horse generally provides remote 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 s knowledge of users who merely visit a malicious or compromised (bugged) 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.

5.6.2 How Malware Affects Systems

Malware poses a significant threat to DHS systems therefore, *it is essential that all systems employ preventive 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 DHS-approved browser configurations should be categorized (trusted, untrusted, etc.). Users must not deploy Web browsers "out of the box," since the security policies implemented in such tools tend to reflect vendor interests that do not coincide with DHS interests.

5.6.3 Procedures When Malware Is Detected On a System

If malware is detected, the LAN/system administrator is responsible for taking appropriate actions, including:

- Running disinfectors available with antivirus software
- Scanning backups for malware prior to restoring system applications and data files
- Checking for re-infection from media overlooked during the eradication process
- Using incident reporting procedures described in Section 4.9 to notify the ISSO of the security incident.
- Once the malicious code has been eradicated, the system administrator determines the extent of the damage and restores the cleaned programs and files to the disinfected system.

Occurrence of malicious code constitutes a *security incident* that must be reported; reporting procedures are described in Section 4.9, "Security Incidents and Incident Response and Reporting."

Virus protection responsibilities are provided in the following table.

Malware Protection Responsibilities
Component CISOs/ISSMs
Establish and enforce malware protection control policy
Provide technical expertise and evaluate the effectiveness of malware protection approaches
Security Control Assessors
Ensure that vulnerability to viruses and other malicious code is detailed in the risk analysis section of the Security Authorization Process 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)
System/Network Administrators
Ensure that all DHS 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 malware prior to use (including blank disks)
Follow procedures detailed in this manual in the event that malware is detected
ISSOs
Employ malware prevention measures commensurate with the level of risk identified 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)
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

Malware Protection Responsibilities
Never disable malware detection software functions Report malware and other malicious code incidents in accordance with procedures described in Section 4.9, Security Incidents and Incident Response and Reporting

5.7 Product Assurance

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

The National Information Assurance Partnership (NIAP) is a collaborative effort by NIST and the NSA designed to meet the security testing, evaluation, and assessment needs of both information system producers and consumers. NIAP combines the extensive security experience of both agencies to promote the development of technically sound security requirements for information system products and appropriate metrics for evaluating those products and systems.

The NIAP Common Criteria Evaluation and Validation Scheme for information security (CCEVS) is a partnership between the public and private sectors, to evaluate information system product conformance to international standards. The scheme is designed to help consumers select products that meet their security requirements while helping the manufacturers of those products gain acceptance in the global marketplace.

Compliance with the DHS 4300A Policy Directive, coupled with the requirement that products have been appropriately validated by designated Federal authorities and by CCEVS, will reduce costs and remove the burden of maintaining and providing interoperability between numerous software systems custom written by various contractors.

Product assurance responsibilities are provided in the following table.

Product Assurance Responsibilities
Component CISO/ISSMs Provide guidance in the use of COTS information assurance products **Security Control Assessors** Validate the proper use of information assurance products **System Administrators/ISSOs** Ensure selected information assurance products are properly deployed and configured **Project Managers** Comply with product assurance policy during system development

5.8 Supply Chain

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.

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.

5.8.1 Business Impact

DHS depends on numerous external supply chains for its ICT needs. Many of these supply chains are independent of one another, and come with their own risks. It is often no longer enough for acquisitions staff to perform due diligence at the beginning of an acquisition. Effective Supply Chain Risk Management (SCRM) requires the analysis of a Business Impact Assessment (BIA) to determine if the supply chain risks represent unacceptable business or mission impact and to propose cost effective counter-measures.

A BIA is most effective at the point in the system acquisition and development lifecycle at which enough is known about the operating environment and interconnections, major components and services, and the allocation of government and contractor responsibilities to determine the likelihood of harm to the enterprise.

5.8.2 SCRM Plans

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 5.8-1.

Figure 5.8-1. SCRM Plan Tiers

5.8.2.1 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 5.8-2 shows graphically how a Tier 3 SCRM plan may evolve over its lifecycle.

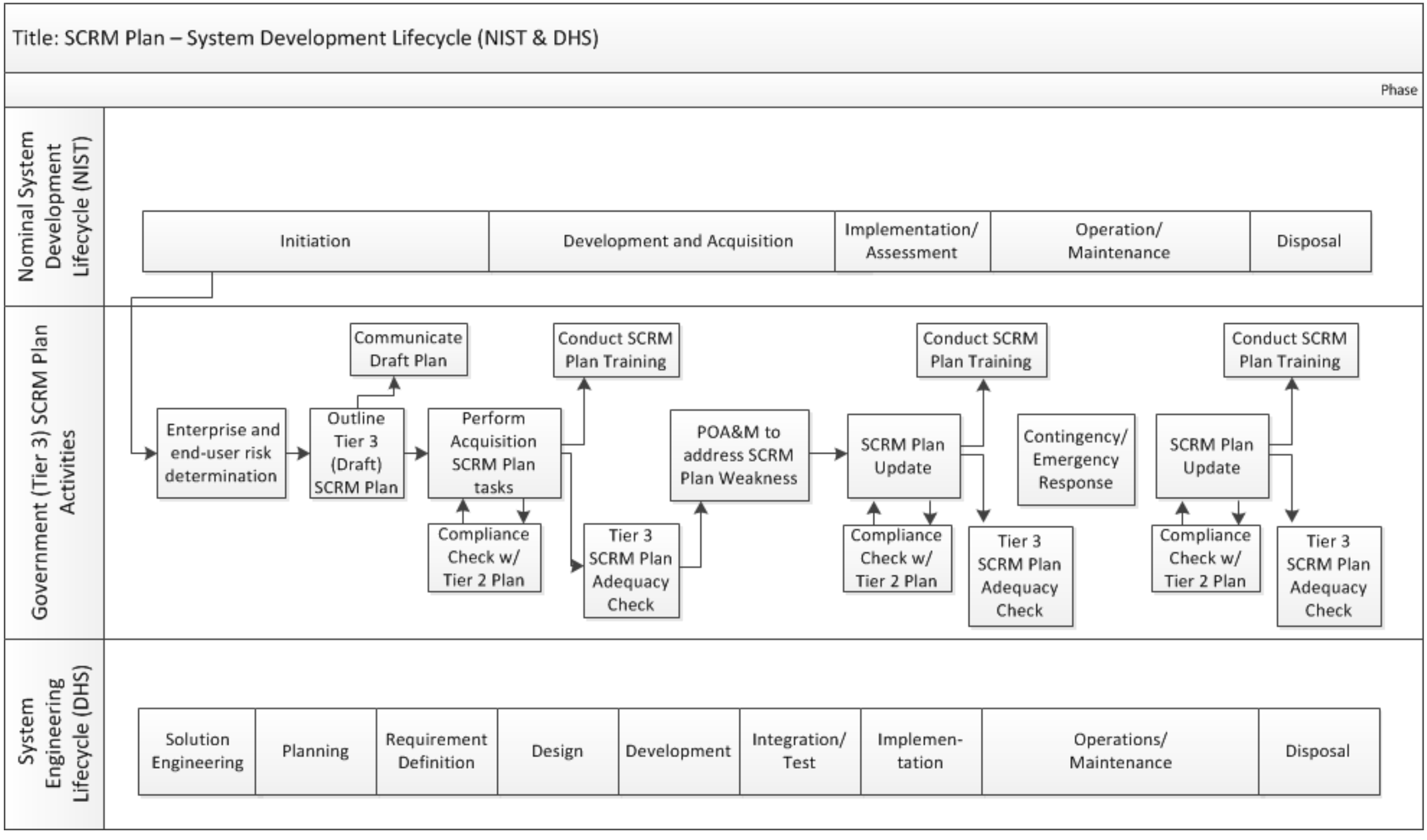


Figure 5.8-2. Nominal SCRM Plan Lifecycle

5.8.2.2 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 Chief Information Security Officer (CISO), 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, 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	Apply SCRM Countermeasures - Require source diversity - Enhanced review of integrators/suppliers - Procure products only through

	Enhancement of Existing Information Assurance Activities	SCRM-Unique
	supply chain elements - 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	manufacturer/vendor-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

Table 5.8-1. Countermeasures Recommendations

6.0 DOCUMENT CHANGE REQUESTS

Changes to "DHS Sensitive Systems Policy Directive 4300A" and to the *DHS 4300A Sensitive Systems Handbook* may be requested in accordance with Section 1.9, "Changes to Policy."

7.0 QUESTIONS AND COMMENTS

For clarification of DHS information security policies or procedures, contact the DHS Director for Information Systems Security Policy at infosecpolicy@hq.dhs.gov.

APPENDIX A ACRONYMS AND ABBREVIATIONS

Acronym	Meaning
3-DES	Triple Data Encryption Standard
ACD	Automatic Call Distribution
AES	Advanced Encryption Standards
AIS	Automated Information System
A-Number	Alien Registration Number
AO	Authorizing Official
APO	Army Post Office
ARB	Acquisition Review Board
ATO	Authority to Operate
BI	Background Investigation
BIA	Business Impact Assessment
BLSR	Baseline Security Requirements
CA	Certification Authority
CBP	Customs and Border Protection
CCB	Change Control Board
CCE	Common Configuration Enumeration
CD	Compact Disk
CFO	Chief Financial Officer
CI	Counter-Intelligence
CIFS	Common Internet File Service
CIO	Chief Information Officer
CISID	Chief, Internal Security and Investigations Division
CISID-OIS	Chief, Internal Security and Investigations Division, Office of Security
CISO	Chief Information Security Officer
CM	Configuration Management
CMG	Core Management Group
CMP	Configuration Management Plan
CO	Continuity of Operations

Acronym	Meaning
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan Continuity of Operations Planning
COTS	Commercial off the Shelf
CP	Contingency Plan Contingency Planning Certificate Policy
CPE	Common Platform Enumeration
CPIC	Capital Planning and Investment Control
CPS	Certificate Practices Statement
CRC	Cyclical Redundancy Check
CRE	Computer-Readable Extract
CRL	Certificate Revocation List
CSID-OIS	Chief, Internal Security and Investigations Division, Office of Security
CSO	Chief Security Officer
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
DES	Digital Encryption Standards
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DNSSEC	Domain Name System Security Extensions
DOD	Department of Defense
DoS	Denial of Service
DoT	Department of Treasury
DR	Disaster Recovery
DT&E	Development Test and Evaluation
DVD	Digital Video Disk
EA	Enterprise Architecture
EAB	Enterprise Architecture Board
EO	Executive Order

Acronym	Meaning
FAM	Foreign Affairs Manual
FBCA	Federal Bridge Certification Authority
FDCC	Federal Desktop Core Configuration (term now obsolete, replaced by U.S. Government Configuration Baseline (USGCB)
FEMA	Federal Emergency Management Agency
FICAM	Federal Identity, Credentialing, and Access Management
FIPS	Federal Information Processing Standard
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
FOIA	Freedom of Information Act
FPGA	Field Programmable Gate Array
FPKI PA	Federal PKI Policy Authority
FTP	File Transfer Protocol
FYHSP	Future Years Homeland Security Program
GSA	General Services Administration
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
HSAR	Homeland Security Acquisition Regulations
HSDN	Homeland Secure Data Network
HSPD	Homeland Security Presidential Directive
HVAC	Heating, Ventilation and Air Conditioning
I&A	Intelligence and Analysis
IA	Identification and Authentication Information Assurance
IACS	Information Assurance Compliance System
IATO	Interim Authority to Operate
IAVA	Information Assurance Vulnerability Assessment
ICAM	Identity, Credentialing, and Access Management
ICAT	Internet Categorization of Attacks Toolkit

Acronym	Meaning
ICE	Immigration and Customs Enforcement
IDF	Intermediate Distribution Frame
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IOC	Initial Operating Capability
IPT	Integrated Product Team
IR	Incident Response Infrared
IRB	Investment Review Board
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISA	Interconnection Security Agreement
ISP	Internet Service Provider
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISVA	Information Security Vulnerability Alert
ISVB	Information Security Vulnerability Bulletin
ISVM	Information System Vulnerability Management
IT	Information Technology
ITAR	Information Technology Acquisition Review
ITGC	Information Technology General Controls
IXC	Inter-exchange Carrier
JWICS	Joint Worldwide Intelligence Communications System
KDP	Key Decision Point
LAN	Local Area Network
LBI	Limited Background Investigation
LE	Law Enforcement
LEC	Local Exchange Carrier
LMR	Land Mobile Radio
MA	Major Application

Acronym	Meaning
MBI	Minimum Background Investigation
MD	Management Directive
MDF	Main Distribution Frame
MMS	Multimedia Messaging Service
MO	Magneto Optical
NAC	National Agency Check
NACIC	National Agency Check and Inquiries and Credit
NACLC	NAC with Law and Credit
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
NLT	No Later Than
NOC	Network Operations Center
NPPD	National Protection and Programs Directorate
NSA	National Security Agency
NSF	Nonstandard Facilities
OCIO	Office of the Chief Information Officer
OID	Object identifier
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPA	Office of Public Affairs
OPM	Office of Personnel Management
OT&E	Operational Test and Evaluation
OTAR	Over-The-Air-Rekeying
PBX	Private Branch Exchange
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications Services
PDA	Personal Digital Assistant

Acronym	Meaning
PED	Portable Electronic Device
PEP	Policy Enforcement Point
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identity Number
PIRT	Privacy Incident Response Team
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PKI PA	PKI Policy Authority
PKI MA	PKI Management Authority
PM	Program Manager
PNS	Protected Network Services
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPOC	Privacy Point of Contact
PSTN	Public Switched Telephone Network
PTA	Privacy Threshold Analysis
RA	Risk Assessment Registration Authority
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFID	Radio Frequency Identification
RMS	Risk Management System
ROB	Riles of Behavior
ROM	Read Only Memory
RTM	Requirements Traceability Matrix
SA	Security Architecture

Acronym	Meaning
SAISO	Senior Agency Information Security Officer
SAN	Subject Alternative Name
SAOP	Senior Agency Official for Privacy
SAR	Security Assessment Report
SCAP	Security Content Automation Protocol
SCI	Sensitive Compartmented Information
SCRM	Supply Chain Risk Management
SELC	Systems Engineering Life Cycle
SFTP	Secure File Transfer Protocol
SIM	Security Incident Management
SLA	Service Level Agreement
SMS	Short Message Service
SOC	Security Operations Center
SOC CONOPS	Security Operations Center Concept of Operations
SORN	System of Records Notice
SOW	Statement of Work
SP	Special Publication (only in titles of NIST publications, e.g. SP 800-37) Security Plan
SSBI	Single Scope Background Investigation
SSH	Secure Shell
SSL	Secure Socket Layer
SSP	Shared Service Provider
Stat.	Statute (refers to a law found in *U.S. Statutes at Large*)
TA	Technical Advisory
~~TAF~~	~~Trusted Agent FISMA~~ [Tool superseded by IACS]
TCP	Transport Control Protocol
TCP/IP	Transport Control Protocol/Internet Protocol
TFPAP	Trust Framework Provider Adoption Process
TIA/EIA	Telecommunications Industry Association/Electronic Industries Alliance
TIC	Trusted Internet Connections

Acronym	Meaning
TOS	Terms of Service
TRM	Technical Reference Model
TS	Top Secret
TS/SCI	Top Secret, Sensitive Compartmented Information
TSA	Transportation Security Administration
UCMJ	Uniform Code of Military Justice
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
USC	United States Code (in citations of codified U.S. law)
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Service
USGCB	U.S. Government Configuration Baseline
USSS	United States Secret Service
VA	Vulnerability Assessment
VAT	Vulnerability Assessment Team
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WORM	Write Once Read Many
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network

APPENDIX B GLOSSARY

The following definitions apply to the policies and procedures outlined in this document. Other definitions may be found in National Institute of Standards and Technology (NIST) IR 7298, "Glossary of Key Information Security Terms" and in the "National Information Assurance (IA) Glossary."

Acceptable Risk	Mission, organizational, or program-level risk deemed tolerable by the Risk Executive after adequate security has been provided.
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. [OMB Circular A-130, Appendix III]
Annual Assessment	Department of Homeland Security (DHS) activity for meeting the annual Federal Information Security Management Act (FISMA) self-assessment requirement.
Authorization Package	The documents submitted to the AO for the Authorization Decision. An Authorization Package consists of: Authorization Decision Letter Security Plan - criteria provided on when the plan should be updated Security Assessment Report - updated on an ongoing basis whenever changes are made to either the security controls in the information system or the common controls inherited by those systems Plan of Action and Milestones (POA&M)
Authorizing Official (AO)	An official within a Federal Government agency empowered to grant approval for a system to operate.
Certification/ Certifying Agent	A contractor that performs certification tasks as designated by the CO.
Certificate (or Certifying) Authority (CA)	A trusted third party that issues certificates and verifies the identity of the holder of the digital certificate.
Chief Information Officer (CIO)	The executive within a Federal Government agency responsible for its information systems.
Compensating Control	An internal control intended to reduce the risk of an existing or potential control weakness.

Component	A DHS Component is any of the entities within DHS, including every DHS office and independent agencies.
Computer Security Incident Response Center	DHS organization that responds to computer security incidents.
Designated Approval Authority (DAA)	Obsolete term; see Authorizing Official (AO).
Enterprise Security Operations Center (SOC)	The DHS organization that coordinates security operations for the DHS Enterprise.
Exception	Acceptance to permanently operate a system that does not comply with policy.
For Official Use Only (FOUO)	The marking instruction or caveat "For Official Use Only" will be used within the DHS community to identify sensitive but unclassifed information that is not otherwise specifically described and governed by statute or regulation.
General Support System (GSS)	An interconnected set of information resources under the same direct management control and sharing common functionality. A GSS normally includes hardware, software, information, applications, communications, data, and users.
Information Security Vulnerability Management (ISVM)	A DHS system that provides notification of newly discovered vulnerabilities, and tracks the status of vulnerability resolution.
Information System	Any information technology that is (1) owned, leased, or operated by any DHS Component, (2) operated by a contractor on behalf of DHS, or (3) operated by another Federal, state, or local Government agency on behalf of DHS. Information systems include general support systems and major applications (MA).
Information System Security Officer (ISSO)	A Government employee or contractor who implements and/or monitors security for a particular system.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Major Application (MA)	An automated information system (AIS) that "requires special attention to security due to the risk and magnitude of harm that can result from the loss, misuse, or unauthorized access to or modification of the information in the application" in accordance with OMB Circular A-130. An MA is a discrete application, whereas a GSS may support multiple applications.
Management Controls	The security controls for an information system that focus on the management of risk and the management of information system security.
Operational Controls	The security controls for an information system that are primarily implemented and executed by people (as opposed to being executed by systems).
Operational Risk	The risk contained in a system under operational status. It is the risk that an AO accepts when granting an ATO.
Personally Identifiable Information (PII)	Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to an individual regardless of whether the individual is a U.S. Citizen, legal permanent resident, or a visitor to the U.S.
Pilot	A test system in the production environment that may contain operational data and may be used to support DHS operations, typically in a limited way.
Policy Enforcement Point (PEP)	A firewall or similar device that can be used to restrict information flow.
Policy Statement	A high-level rule for guiding actions intended to achieve security objectives.
Portable Electronic Device (PED)	A device that has a battery and is meant to process information without being plugged into an electric socket; it is often handheld but can be a laptop computer.
Privacy Sensitive System	Any system that collects, uses, disseminates, or maintains PII or sensitive PII.
Privileged Network User	A user that is authorized (and, therefore, trusted) to perform security-relevant functions for purposes including but not limited to network system administration, security policy and procedure management, and system maintenance and controls.
Production	The applications and systems that DHS end users access and use operationally to execute business transactions.
Prototype	A test system in a test environment that must not contain operational data and must not be used to support DHS operations.

Remote Access	Access to a DHS information system by a user (or an information system) communicating through an external, non-DHS-controlled network (e.g., the Internet).
Residual Risk	The risk remaining after security controls have been applied.
Risk Executive (RE)	An individual who ensures that risks are managed consistently across the organization. An RE can be at the Departmental or Component level.
Security Control	A particular safeguard or countermeasure to protect the confidentiality, integrity, and availability of a system and its information.
Security Control Assessor	A senior management official who certifies the results of the security control assessment. He or she must be a Federal Government employee.
Security Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Security Operations Center (SOC)	The organization in each DHS Component that coordinates the Component's security operations.
Security Requirement	A formal statement of action or process applied to an information system and its environment in order to provide protection and attain security objectives. Security requirements for any given system are contained in its Security Plan.
8.0 Senior Agency Information Security Official (SAISO)	The point of contact within a Federal Government agency responsible for its information system security.
Sensitive But Unclassified	Obsolete designation; see Sensitive Information.
Sensitive Information	Information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal Government programs or other programs or operations essential to the national interest.
Sensitive Personally Identifiable Information (Sensitive PII)	PII that requires stricter handling guidelines because of the nature of the data and the increased risk to an individual if compromised, and if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of sensitive PII include Social Security numbers and Alien Registration Numbers (A-number).

Significant Incident	A computer security-related incident that represents a meaningful threat to the DHS mission and requires immediate leadership notification.
Spam	Emails containing unwanted commercial solicitation, fraudulent schemes, and possibly malicious logic.
Strong Authentication	Layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information.
System	A discrete set of information system assets contained within the authorization boundary.
System Owner	The agency official responsible for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.
Technical Controls	The security controls for an information system that are primarily implemented and executed by the information system through mechanisms contained in system hardware, software, or firmware.
Two-Factor Authentication	Authentication can involve something the user knows (e.g., a password), something the user has (e.g., a smart card), or something the user "is" (e.g., a fingerprint or voice pattern). Single-factor authentication uses only one of the three forms of authentication, while two-factor authentication uses any two of the three forms. Three-factor authentication uses all three forms.
Unclassified Information	Information that has not been determined to be classified pursuant to Executive Order 13526, as amended.
USB Device	A device that can be connected to a computer via a USB port.
USB Drive	A memory device small enough to fit into a pocket that connects to a computer via a USB port.
Vulnerability Scanning	An automated scan for potential security vulnerabilities.
Waiver	Temporary dispensation of a policy requirement, granted to a Component to operate a system while working toward compliance.

APPENDIX C REFERENCES

The DHS information security program and organization are based upon public laws, executive orders, national policy, external guidance, and internal DHS guidance.

Public Laws and U.S. Code

- Privacy Act of 1974, as amended, Public Law 93-579, codified at 5 USC 552a
- E-Government Act of 2002, including Title III, Federal Information Security Management Act (FISMA), Public Law 107-347, codified at 44 USC. §§ 3541-3549
- Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], Public Law 104-106, codified at 5 CFR*CFR* § 2635, Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch
- Computer Security Act of 1987 as amended, Public Law 100-235, codified at 40 USC 759.
- Freedom of Information Act of 2002, as amended, Public Law 89-554, 80 Stat 383, amended 1996, 2002, 2007

Executive Orders

- Executive Order 12958, "Classified National Security Information," March 25, 2003
- Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004

Office of Management and Budget Directives

- Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," revised, November 30, 2000
- OMB Bulletin 06-03, "Audit Requirements for Federal Financial Statements," August 23, 2006
- 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 Management Act and Agency Privacy Management, April 21, 2010

- OMB Memorandum 10-28, "Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)," July 6, 2010
- OMB Memorandum 11-06, "WikiLeaks - Mishandling of Classified Information," November 28, 2010

Other External Guidance

- Intelligence Community Directive Number 508, "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:
    - NIST FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006"
    - NIST FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004
- NIST Information Technology Security Special Publications (SP) 800 series, including:
    - NIST SP 800-16, Rev 1, "Information Technology Security Training Requirements: A Role- and Performance-Based Model (Draft)," April 1998
    - 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," May, 1010
    - NIST SP 800-37, Rev 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 2010
    - NIST SP 800-39, "Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View," March 2011
    - NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program," October 2003
    - NIST SP 800-52, "Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations," June 2005
    - NIST SP 800-53, Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013, with updates as of January 15, 2014
    - NIST SP 800-53A, Rev 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans," June 2010
    - NIST SP 800-60, Rev 1, "Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices," August 2008

- NIST SP 800-63, Rev 1, Draft 3"Electronic Authentication Guideline, June 2011
- NIST SP 800- 65, Rev 1, Draft, "Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process (CPIC)," July 14, 2009
- NIST SP 800-88, "Guidelines for Media Sanitization," Sept 2006
- NIST SP 800-92, "Guide to Computer Security Log Management," September 2006
- 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 800-100, "Information Security Handbook: A Guide for Manager," October 2006
- NIST SP 800-115, "Technical Guide to Information Security Testing and Assessment," November 2008
- NIST SP 800-118, Draft, "Guide to Enterprise Password Management (Draft)," April 21, 2009
- 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, "Guidelines on Cell Phone and PDA Security," October 2008
- NIST SP 800-128, "Guide for Security Configuration Management of Information Systems (Draft)," August 2011
- NIST SP 800-137, "Information Security Continuous Monitoring for Federal Information Systems and Organizations," September 2011

- NIST Interagency or Internal Reports (NISTIR)
  - NIST IR 7298 Rev 1, "Glossary of Key Information Security Terms," February 2011
- Committee on National Security Systems (CNSS) Instructions
- CNSS Instruction No. 4009 (Revised), "National Information Assurance Glossary," April 2010
- CNSS Instruction No. 1001, "National Instruction on Classified Information Spillage," February 2008

Internal Guidance

- "Department of Homeland Security Acquisition Regulation (HSAR)," 48 CFR Chapter 30, June 2006
- DHS Privacy Incident Handling Guidance, January 2012

- **DHS Management Directives (MD), especially**:
  - Directive 047-01, "Privacy Policy and Compliance," July 7, 2011
  - MD 140-01, "Information Technology Systems Security," July 31, 2007
  - MD 11042.1,"Safeguarding Sensitive but Unclassified (For Official Use Only) Information." January 6, 2005
  - MD 1030, "Corrective Action Plans," May 15, 2006
  - MD 4400.1, **DHS Web** (Internet, Intranet, and Extranet Information) and Information Systems," March 1, 2003
  - MD 4500.1, "DHS Email Usage," 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," document undated
- DHS Instruction 121-01-007," Personnel Suitability and Security Program," June 2009
- DHS Directive 102-01, "Acquisition Management," January 20, 2010

APPENDIX D DOCUMENT CHANGE HISTORY

Version	Date	Description
0.1	December 13, 2002	Draft Baseline Release
0.2	December 30, 2002	Revised Draft
0.5	January 27, 2003	Day One Interim Policy
1.0	June 1, 2003	Department Policy
1.1	December 3, 2003	Updated Department Policy
2.0	March 31, 2004	Content Update
2.1	July 26, 2004	Content Update
2.2	February 28, 2005	Content Update
2.3	March 7, 2005	Content Update
3.0	March 31, 2005	Includes updates to PKI, Wireless Communications, and Media Sanitization (now Media Reuse and Disposition) sections
3.1	July 29, 2005	New policies: 3.1b,e,f, 3.1g. 4.1.5b, 4.8.4a. Modified policies: 3.7b, c, 3.9b,g, 3.10a, 4.3.1b, 4.8.2a, 4.8.5e, 5.1.1b, 5.2.2a, 5.3a, c, 5.4.1a, 5.4.5d, 5.4.8c, 5.5.1a, 5.7d. Policies relating to media disposal incorporated into policies within Media Reuse and Disposition section. Deleted policy regarding use of automated DHS tool for conducting vulnerability assessments.
3.2	October 1, 2005	Modified policies 3.8b, 4.8.1a, 5.2.1a&b, 5.2.2a, and 5.4.3c; combined (with modifications) policies 4.1e and 4.1f; modified Section 1.5
3.3	December 30, 2005	New policies: policies 3.9a–d; 3.11.1b; 4.3.1a; 4.6c; 5.4.3d&e. Modified policies: policies 3.9i&j; 4.3.2a; 4.6a, b; 4.6.1e; 4.6.2j; 4.6.2.1a; 4.6.3e; 5.4.3c; 5.5.2k. Modified sections: 2.5, 2.7, 2.9, 2.11, 3.9, 5.5.2.
4.0	June 1, 2006	New policies: 3.5.3.c&g, 4.6.2.3.c, 5.1.c, 5.2.c, 5.4.1.a. Modified policies: 3.5.1.c, 3.5.3.d–f, 3.7.a&b, 3.9.a&b, d, 4.1.4.b&c, 4.2.1.a, 4.3.1.a, 4.6.c, 4.6.1.a, 4.6.2.f, 4.10.3.a, 5.2.1.b, 5.3.a&b, 5.4.1.b, 5.4.3.c, 5.4.5.d. Modified section: Section 2.9.
4.1	September 8, 2006	New policies: 3.14.1.a–c; 3.14.3.a–c; 4.10.1.c; 5.3.d&e; 5.4.1.c–e. Modified policies: 3.9.b; 4.6.2.d; 4.8.2.a–c; 4.10.1.b; 5.1.c; 5.3.c; 5.4.1.b. New sections: 3.14, 3.14.1, 3.14.3. Modified sections: 2.9, 4.8.2.
4.2	September 29, 2006	New policies: 4.6.4.a–f. Modified policies: 4.3.3.a–c. New section: 4.6.4.
5.0	March 1, 2007	New policies: 4.1.5.h. Modified policies: 3.10.c, 4.1.1.d, 4.1.5.a,b,f, &g,

Version	Date	Description
		4.6.2.d, 4.6.3.f, 5.2.c, 5.4.8.a, 5.6.b. New sections: 4.1.1. Modified sections: 1.2, 1.4.2, 1.4.3, 2.9, 3.12, 4.1 and subsections, 4.6.1–4.6.4, 4.9, 5.2.1. Renumbered sections: 4.1.2–4.1.6, 4.9, 4.10, 4.11, 4.12.
5.1	April 18, 2007	Update based on SOC CONOPS, Final Version 1.4.1, April 6, 2007; Adds DHS Chief Financial Officer – Designated Financial Systems; Updates the term, *Sensitive But Unclassified* to *For Official Use Only*
5.2	June 1, 2007	Updates Sections 2.7, 2.9, 2.12, 3.3, 3.5.1, 3.5.3, 3.6, 3.8, 3.9, 3.10, 3.14, 3.15, 4.1.5, 4.1.6, 4.10, 4.12, 5.1.1, 5.2, 5.3, 5.4.1, 5.4.3, 5.4.4, 5.4.8, 5.5.1, 5.7
5.3	August 3, 2007	Revised policy in Sections 3.5.1 and 5.5.1, and removed Section 3.5.2. Removed Sections 3.11.2 and 3.11.4
5.4	October 1, 2007	Content update, incorporation of change requests
5.5	September 30, 2007	**Section 1.0:** 1.1 – Added text regarding policy implementation and DHS security compliance tool updates. 1.2 – Removed two references from list; deleted "various" from citation of standards. **Section 2.0:** 2.0 – Insert the following after the first sentence in the second paragraph: “Security is an inherently governmental responsibility. Contractors and other sources may assist in the performance of security functions, but a government individual must always be designated as the responsible agent for all security requirements and functions.” 2.3 – Removed parentheses from "in writing." **Section 3.0:** 3.9 – Inserted new policy element “l” regarding CISO concurrence for accreditation. 3.15 – Added text regarding Component CFOs and ISSMs. **Section 4.0:** 4.1.1 – Capitalized “Background,” and added "(BI)." 4.3.1 – Two new elements were added to the policy table. 4.7 – Inserted "where required or appropriate" before the sentence. 4.8.3 – Title changed to “Personally Owned Equipment and Software (not owned by or contracted for by the Government).” 4.8.6 – Included new section regarding wireless settings for peripheral equipment. **Section 5.0:** 5.1c – Changed inactive accounts to “disable user identifiers after 45 days of inactivity.” 5.1.1 – First sentence of the second paragraph was rewritten to prohibit use of personal passwords by multiple individuals. 5.2.2 – Title changed to “Automatic Session Termination.”
6.0	May 17, 2008	**Global change** “Shoulds” changed to “shalls” throughout the document. Replaced certain instances of “will” with “shall” throughout document to indicate compliance is required. Various changes were made throughout the document to ensure that the 4300A Policy and Handbook align with the 4300B Policy and Handbook. “ISSM” changed to “CISO/ISSM” throughout the document. "CPO" changed to "Chief Privacy Officer" throughout the document.

Version	Date	Description
		"IT Security Program" changed to "Information Security Program" throughout the document." "System Development Life Cycle" changed to "System Life Cycle" and "SDLC" changed to "SLC" throughout the document. **Title Page** Title page of 4300A Policy - Language on the Title Page was reworded. "This is the implementation of DHS Management Directive 4300.1." **Section 1.0** 1.1 – Updated to clarify 90 day period in which to implement new policy elements. 1.2 – Added OMB, NIST, and CNSS references. 1.4 – Added reference and link to Privacy Incident Handling Guidance and the Privacy Compliance documentation. 1.4.2 – Added definition of National Intelligence Information. 1.4.3 – Inserted definition of National Security Information to align with 4300B Policy. 1.4.8.1 – Definition of General Support System was updated. 1.4.8.2 – Definition of Major Application was updated. 1.4.10 – Section was renamed "Trust Zone." 1.4.16 – Inserted new definition for FISMA. 1.5 – Language was updated to increase clarity for financial system owners for waivers and exceptions. **Section 2.0** 2.3 – Added a new responsibility for DHS CIO. 2.4 – Added a new responsibility for Component CIOs. 2.5 - Chief Information Security Officer (CISO) renamed DHS Chief Information Security Officer (CISO). Updated to include privacy-related responsibilities. 2.6 – Added a new section in Roles and Responsibilities called "Component CISO." 2.7 – Updated Component ISSM Role and Responsibilities. 2.8 – Changed name of the section from "Office of the Chief Privacy Officer (CPO)" to "The Chief Privacy Officer". Updated to include privacy-related responsibilities. 2.9 – Added a new role for DHS CSO. 2.10 – Updated to include privacy-related responsibilities. 2.11 - Added privacy-related responsibilities. 2.12 – Added a new section, "OneNet Steward." 2.13 – Added a new section, "DHS Security Operations Center (DHS SOC)

Version	Date	Description
		and Computer Security Incident Response Center (CSIRC)." 2.14 – Added a new section, "Homeland Secure Data Network (HSDN) Security Operations Center (SOC)." 2.16 – Added a new section, "Component-level SOC." 2.18 – Updated to include privacy-related responsibilities. 2.19 – Last sentence of first paragraph has been updated to say: "ISSO Duties shall not be assigned as a collateral duty. Any collateral duties shall not interfere with their ISSO duties." 2.20 – Updated to include privacy-related responsibilities. **Section 3.0** 3.9 – Added C&A information for unclassified, collateral classified and SCI systems. Also, prior to DHS Policy table, included sentence regarding C&A. 3.9.b – Language updated to clarify that a minimum impact level of moderate is required for confidentiality for CFO designated financial systems. 3.9.h – New guidance is provided to clarify short term ATO authority. 3.11.1 – Added new section discussing the CISO Board. 3.11.3 – Removed DHS Wireless Security Working Group. 3.14.1 – Added new text defining PII and sensitive PII. At the end of bullet #4, added definition of computer-readable data extracts. Updated 3.14.1.a and 3.14.1.b based on input from the Privacy Office. Added sentence "DHS 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. 3.14.2 - Added new section called "Privacy Threshold Analyses." 3.14.3 - Updated Privacy Impact Assessment Responsibilities table. 3.14.4 - Added new section called "System of Record Notices." **Section 4.0** 4.1.5.c – Updated to address training requirements. 4.1.5.g – Deleted "Training plans shall include awareness of internal threats and basic IT security practices." 4.1.5.h (now 4.1.5.g) – Updated to include the following sentence: "Components shall account for Contingency Plan Training, and Incident Response Training conducted for Moderate and High IT Systems." 4.3.1.d – FIPS 140-2 compliance language was updated. 4.8.1.a and 4.8.1.c – Language has been updated to provide clarification of timeout values. 4.8.2.a – FIPS 140-2 compliance language was updated. 4.8.2.b – Added a new policy element regarding powering down laptops when not in use.

Version	Date	Description
		4.9 – Section was renamed "Department Information Security Operations." 4.9, 4.9.1, 4.9.2 – Updated policy elements to support Department security operations capabilities, based on the SOC CONOPS. 4.9.2.b – Updated to say "Components shall obtain guidance from the DHS SOC before contacting local law enforcement except where there is risk to life, limb, or destruction of property." 4.12.a – Added policy element to align with Handbook. **Section 5.0** 5.2.1.a, 5.2.1.b, and 5.2.1.c – Language has been updated to provide clarification of timeout values. 5.2.2 Introductory language, 5.2.2.a, 5.2.2.b, and 5.2.2.c – Language and policy updated to clarify the meaning of a session termination. 5.3.f - Updated to clarify responsibilities of the System Owner regarding computer-readable data extracts. 5.4.1.d – Added sentence "DHS 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." 5.4.3.a through i – New guidance is provided regarding the preparation of ISAs for interconnections to the DHS OneNetwork. 5.4.3.g – Replaced "interconnect service agreements" with "interconnection security agreements." 5.4.4.f - New guidance is provided regarding internal firewalls. 5.4.5.f – New guidance is provided regarding the use of the RDP protocol. 5.4.6 – Added text "NOTE: Due to many attacks that are HTML-based, please note that DHS will be following the lead of the DoD and moving to text based email." 5.4.8.a – Language updated to reflect that annual vulnerability assessments should be conducted. 5.4.8.f – Policy updated to clarify automated system scanning. 5.5.1.c – Updated element to specify usage of cryptographic modules that "are FIPS 197 compliant and have received FIPS 140-2 validation." 5.5.2.f – Policy updated to clarify hosting of DHS Root CA.
6.1	September 23, 2008	**Global Changes** Replaced all instances of "CISO/ISSM" with "Component CISO/ISSM." Replaced all DHS-related instances of "agency/agency-wide" with "Department/Department-wide." Replaced all instances of "24x7" with "continuous" or "continuously," as appropriate. Replaced all instances of "IT security" with "information security." Various minor editorial and grammatical changes were made throughout the document.

Version	Date	Description
		Section 1.0 1.2 – Added reference to E-Government Act of 2002, January 7, 2003. 1.4 – Replaced "National InfoSec Glossary" with "National Information Assurance (IA) Glossary." 1.4.5 – Replaced third sentence with "System vulnerability information about a financial system shall be considered Sensitive Financial Information." 1.5.2 – Added text regarding acceptance of resulting risk by the Component CFO for financial systems. 1.5.3 – Corrected the title and location of Attachment B. Added text regarding PTA requirements. **Section 2.0** 2.1 – Updated to clarify Secretary of Homeland Security responsibilities. 2.2 – Updated to clarify Undersecretaries and Heads of DHS Components responsibilities. 2.3 – Updated to clarify DHS CIO responsibilities. 2.4 – Updated to clarify Component CIO responsibilities. 2.5 – Updated to clarify DHS CISO responsibilities. 2.6 – Updated to clarify Component CISO responsibilities. 2.8 – Moved "The Chief Privacy Officer" section to 2.9. 2.11 – Updated to clarify Program Managers' responsibilities. 2.14 – Updated to clarify HSDN SOC responsibilities. Updated HSDN SOC unclassified email address. 2.19 – Updated to clarify ISSO responsibilities and the assignment of ISSO duties as a collateral duty. 2.20 – Updated to clarify System Owners' responsibilities. 2.23.2 – Updated to clarify DHS CIO responsibilities for financial systems. **Section 3.0** 3.1.e – Replaced "FISMA and OMB requirements" with "FISMA, OMB, and other Federal requirements." 3.1.h – Replaced "maintain a waiver" with "maintain a waiver or exception." 3.14.1 – Included text regarding the type of encryption needed for laptops. 3.14.3 – Included text stating that the PTA determines whether a PIA is conducted. 3.14.4 – Moved first sentence of second paragraph to be the first sentence of the first paragraph. Included "that are a system of record" after "IT Systems" in the second sentence of the first paragraph. **Section 4.0** 4.3.1.a – Included "locked tape device" in media protection.

Version	Date	Description
		4.3.1.d – Updated to clarify that AES 256-bit encryption is mandatory. 4.8.2.a – Updated to clarify that AES 256-bit encryption is mandatory. 4.8.3.c – Included new policy element regarding use of seized IT equipment. 4.8.4.f – Included new policy element regarding management and maintenance of system libraries. 4.8.5.b – Policy updated to clarify limited personal use of DHS email and Internet resources. 4.9 – First paragraph updated to clarify DHS SOC and HSDN SOC responsibilities. 4.9.b – Updated to specify that the HSDN SOC is subordinate to the DHS SOC. 4.9.1 – First two paragraphs updated to clarify relationship between the DHS SOC and the HSDN SOC. 4.9.1.a – Removed the words "Component SOC." 4.9.1.b – Updated to clarify means of communication for reporting significant incidents. 4.9.1.c – Updated to clarify the length of time by which significant HSDN incidents must be reported. 4.9.1.d. – Updated to clarify reporting for HSDN incidents. **Section 5.0** 5.2.d – Replaced "Component CISO/ISSM" with "Component CISO/ISSM or his/her designee." 5.2.1 – Changed "48 hour time period" to "24 hour time period." 5.4.5.g – Included new policy element regarding blocking of specific Internet websites or categories. 5.4.7 – Updated the policy element to prohibit use of webmail and other personal email accounts. 5.5.1.c – Updated to clarify that AES 256-bit encryption is mandatory. 5.7.d – Included new policy element regarding use of cryptographic modules in order to align with 4300A Handbook. 5.7.e – Included new policy element regarding rollback and journaling for transaction-based systems.
6.1.1	October 31, 2008	5.2.3 – Included new language and a link to the DHS computer login warning banner text on DHS Online.
7.0		**General Updates** Added section and reference numbers to policy elements Added NIST 800-53 reference controls to policy elements Added hyperlinks to most DHS references Introduced new terminology Senior Agency Information Security Officer, Risk Executive, and Authorizing Official (AO) – replaces DAA, as per NIST 800-37 and 800-53

Version	Date	Description
		Added Appendix A – Acronyms Added Appendix B – Glossary Added Appendix C – References list has been updated and moved to Appendix C. (these are detailed references, an abbreviated list is still found at the beginning of the document) Added Appendix D – Change History (This was moved from the front of the document) **Specific Updates** **Section 1.1 – Information Security Program Policy** – Added the statement, "Policy elements are designed to be broad in scope. Specific implementation information can often be found in specific National Institute for Standards and Technology (NIST) publications, such as NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Systems." **Section 1.4.17-19 – Privacy** – Added definitions for PII, SPII, and Privacy Sensitive Systems **Section 1.5 – Exceptions and Waivers** – Updated this section, clarified policy elements, and consolidated all exceptions and waivers requirements. **Section 1.5.4 – U.S. Citizen Exception Requests** – Updated section to include policy elements: 1.5.4.a – Persons of dual citizenship, where one of the citizenships includes U.S. Citizenship, shall be treated as U.S. Citizens for the purposes of this directive. 1.5.4.b – Additional compensating controls shall be maintained for foreign nationals, based on nations lists maintained by the DHS CSO. **Section 1.6 – Information Sharing and Communication Strategy** – Added policy element: 1.6.a - For DHS purposes, electronic signatures are preferred to pen and ink or facsimile signatures in all cases except where pen & ink signatures are required by public law, Executive Order, or other agency requirements. **Section 1.7 – Changes to Policy** – Updated entire section **Section 2.0 – Roles and Responsibilities** – Reformats entire section. Places emphasis on DHS CISO and Component-level Information Security Roles. Secretary and senior management roles are moved to the end of the section. Some specific areas to note include: **Section 2.1.1 – DHS Senior Agency Information Security Officer** – Introduces this term and assigns duties to DHS CISO **Section 2.1.2 – Chief Information Security Officer** – Adds the following responsibilities: - Appoint a DHS employee to serve as the Headquarters CISO - Appoint a DHS employee to serve as the National Security Systems (NSS) CISO **Section 2.1.3 – Component Chief Information Security Officer** – Adds policy element: 2.1.3.b - All Components shall be responsible to the appropriate CISO.

Version	Date	Description
		Components without a fulltime CISO shall be responsible to the HQ CISO. Adds 4 additional CISOs to the list of Component CISOs: Federal Law Enforcement Training Center Office of the Inspector General Headquarters, Department of Homeland Security The DHS CISO shall also appoint an NSS CISO **Section 2.1.4 – Component Information Systems Security Manager** – Component CISO now works directly with the HQ CISO, rather than with the DHS CISO. **Section 2.1.5 – Risk Executive** – Introduces this term as per NIST. Assigns responsibilities to CISOs (already performing these functions) **Section 2.1.6 – Authorizing Official** – Introduces this term as per NIST. Replaces the term Designated Approval Authority (DAA) **Section 2.2.10 – DHS Employees, Contractors, and Vendors** – Adds the requirement for vendors to follow DHS Information Security Policy **Section 3.2 – Capital Planning and Investment Control** – Adds policy element: 3.2.f – Procurement authorities throughout DHS shall ensure that Homeland Security Acquisition Regulation (HSAR) provisions are fully enforced. **Section 3.3 – Contractors and Outsourced Operations** – Adds policy element: 3.3.g – Procurement authorities throughout DHS shall ensure that Homeland Security Acquisition Regulation (HSAR) provisions are fully enforced. **Section 3.5.2 – Contingency Planning** – Updates and expands entire section. **Section 3.5 – Configuration Management** – Adds policy elements Section 3.7.f – If the information system uses operating systems or applications that do not have hardening or do not follow configuration guidance from the DHS CISO, the System Owner shall request an exception, including a proposed alternative secure configuration. Section 3.7.g – Components shall ensure that CM processes under their purview include and consider the results of a security impact analysis when considering proposed changes. **Section 3.9 – Certification, Accreditation, and Security Assessments** – Updates entire section **Section 3.9.1 – FIPS Categorization and NIST SP 800-53 Controls** – Removed table of controls and referred reader to Attachment M. **Added Section 3.9.10** – Plan of Actions and Milestones and renumbered Sections 3.9.10-11 to 3.9.11-12 **Section 3.11.1 – CISO Council** – Updates the term from CISO Board **Section 3.14-3.14.6 – Privacy Sections** – Updates all sections pertaining to privacy and privacy information, adds section 3.14.5 – Protecting Privacy Sensitive Systems **Section 3.14.7 – E-Authentication** – Renumbers this section from 3.14.6

Version	Date	Description
		(due to adding of privacy section 3.14.5 **Section 3.15 – DHS Chief Financial Officer Designated Systems** – Section renamed from DHS Chief Financial Officer Designated Financial Systems **Section 3.16 – Social Media** – Added Social Media section to provide guidelines and address the Federal Government's (including DHS) use of social media sites (You Tube, Twitter, etc) **Section 4.1.2 – Rules of Behavior** – Added policy element: 4.1.2.b – Components shall ensure that DHS users are trained regarding rules of behavior and that each user signs a copy prior to being granted user accounts or access to information systems or data. **Section 4.1.5 – IT Security Awareness, Training, and Education** – Updates entire section **Section 4.1.6 – Separation from Duty** – Updates policy element to require that all assets and data are recovered from departing individuals 4.1.6.b – Components shall establish procedures to ensure that all DHS information system-related property and assets are recovered from the departing individual and that sensitive information stored on any media is transferred to an authorized individual. Adds policy elements: 4.1.6.c - Accounts for personnel on extended absences shall be temporarily suspended. 4.1.6.d – System Owners shall review information system accounts supporting their programs at least annually. **Section 4.3.2 – Media Marking and Transport** – Adds "Transport" to section title and adds policy element: 4.3.2.b – Components shall control the transport of information system media containing sensitive data, outside of controlled areas and restrict the pickup, receipt, transfer, and delivery to authorized personnel. **Section 4.6 – Wireless Network Communications** – Updated section title from "Wireless Communication" and specifies "network communication" technologies in policy, rather than the more general "Wireless." Removes references to the defunct "WMO." **Section 4.6.1 – Wireless Systems** – Adds policy elements: 4.6.1.f – Component CISOs shall review all system applications for wireless usage, maintain an inventory of systems, and provide that inventory to the DHS CISO at least annually. 4.6.1.g – Component CISOs shall (i) establish usage restrictions and implementation guidance for wireless technologies; and (ii) authorize, monitor, and control wireless access to DHS information systems. **4.9.1 – Security Incidents and Incident Response and Reporting** – Adds requirement for Components to maintain full SOC and CSIRC capability (May outsource to DHS SOC). Adds policy elements: 4.9.1.k – Components shall maintain a full SOC and CSIRC capability or

Version	Date	Description
		outsource this capability to the DHS SOC. The DHS SOC shall provide SOC and CSIRC services to Components in accordance with formal agreements. Information regarding incident response capability is available in Attachment F of the DHS 4300A Sensitive Systems Handbook. 4.9.1.q – The DHS CISO shall publish Incident Response Testing and Exercise scenarios as required. 4.9.1.r – The Component CISO for each Component providing an incident response capability shall ensure Incident Response Testing and Exercises are conducted annually in coordination with the DHS CISO. **Section 5.1 – Identification and Authentication** – Adds requirement for strong authentication following HSPD-12 implementation. 5.1.f – Components shall implement strong authentication on servers, for system administrators and significant security personnel, within six (6) months of the Component's implementation of HSPD-12. **Section 5.4.1 – Remote Access and Dial-In** – Updates section and adds policy element: 5.4.1.f – The Public Switched Telephone Network (PSTN) shall not be connected to OneNet at any time. **5.4.3 – Network Connectivity** – Requires DHS CIO approval for all network connections outside of DHS. Also specifies requirement for CCB. 5.4.3.g – The DHS CIO shall approve all interconnections between DHS information systems and non-DHS information systems. Components shall document interconnections with an ISA for each connection. The DHS CIO shall ensure that connections with other Federal Government Agencies are properly documented. A single ISA may be used for multiple connections provided that the security accreditation is the same for all connections covered by that ISA. 5.4.3.l - The appropriate CCB shall ensure that documentation associated with an approved change to an information system is updated to reflect the appropriate baseline. DHS systems that interface with OneNet shall also be subject to the OneNet CCB. **Section 5.4.4 – Firewalls and Policy Enforcement Points** – Updates language to include Policy Enforcement Points. Adds policy elements: 5.4.4.i – The DHS CISO shall establish policy to block or allow traffic sources and destinations at the DHS TIC PEPs. The DHS CISO policy will prevent traffic as directed by the DHS CIO. 5.4.j – The DHS SOC shall oversee all enterprise PEPs. **Section 5.4.5 – Internet Security** – Prohibits Public Switched Telephone Network (PSTN) connection to OneNet. 5.4.5.a – Any direct connection of OneNet, DHS networks, or DHS mission systems to the Internet or to extranets shall occur through DHS Trusted Internet Connection (TIC) PEPSs. The PSTN shall not be connected to OneNet at any time. **Section 5.5.3 – Public Key/Private Key** – Assigns responsibility for non-human use of PKI to sponsors.

Version	Date	Description
		5.5.3.g – Sponsors for non-human subscribers (organization, application, code-signing, or device) shall be responsible for the security of and use of the subscriber's private keys. Every sponsor shall read, understand, and sign a "DHS PKI Subscriber Agreement for Sponsors" as a pre-condition for receiving certificates from a DHS CA for the non-human subscriber. **Section 5.4.6 – Email Security** – Prohibits auto-forwarding of DHS email to other than .gov addresses. 5.4.6.i - Auto-forwarding or redirecting of DHS email to address outside of the .gov domain is prohibited and shall not be used. Users may manually forward individual messages after determining that the risk or consequences are low. **Section 5.6 – Malware Protection** – Updates term from "Virus."
7.1	September 30, 2009	**General Updates** Standardized the term "IT system" to "information system" Standardized the term "DHS IT system" to "DHS information system" Updated the term "DHS Security Operations Center" to "DHS Enterprise Operations Center" and added definition in glossary Replaced "must" with "shall" in all policy statements Replaced "vendors" with "others working on behalf of DHS" **Specific Updates** **Section 1.4.20** – Strong Authentication – Added definition for Strong Authentication **Section 1.4.21** – Two-Factor Authentication – Added definition for Two-Factor Authentication **Section 2.2.4** – Component Chief Information Officer – Alleviated confusion regarding Component CIO responsibilities **Section 2.2.5** – Chief Security Office – Removed erroneous CSO responsibilities which belong to Component CIOs **Section 2.2.7** – DHS Chief Financial Officer – Updated policy elements to clarify applicable policies **Section 3.1** – Basic Requirements (3.1.d, 3.1.g-j) – Updated policy elements to CISO/ISSM/ISSO responsibilities **Section 3.7.f** – Clarified Operating system exception requirements **Section 3.9.l-m** – Clarified requirements regarding TAF/RMS **Section 3.15** – CFO Designated Systems – Major revisions to this section **Section 4.2.**6 and 5.4.1.a – Prohibits tethering to DHS devices **Section 5.4.3.g-h** – Clarifies interconnection and ISA approval **Section 5.5** – Cryptography – Removed unnecessary elements from introductions and updated entire section with input from DHS PKI Steward
7.2	June 21, 2010	**General Updates**

Version	Date	Description
		No general updates with this revision. Specific updates are listed below. **Specific Updates** **Section 1.4.8** – Added FISMA language (transmits, stores, or processes data or information) to definition of DHS System **Section 1.5.3.k** – Removed requirement for Component Head to make recommendation regarding waivers; removed requirement to report *exceptions* on FISMA report. **Section 2.1.6** – Adds requirement for AO to be a Federal employee **Section 2.1.7** – Clarifies that CO is a senior management official; stipulates that CO must be a Federal employee **Section 2.2.5** – Updated CSO role **Section 3.2** – Added intro to CPIC section **Section 3.5.2.h** – Added requirement to coordinate CP and COOP testing moderate and high FIPS categorizations **Section 3.15.a** – Added requirement for CFO Designated Systems security assessments for key controls be tracked in TAF and adds requirement for tracking ST&E and SAR annually. **Section 3.15.c** – Remaps control from RA-4 to RA-5 **Section 3.15.h** – Adds mapping to IR-6 **Section 3.15.i** – Remaps control from PL-3 to PL-2 **Section 3.17** – Added requirement to protect HIPPA information **Section 3.9.8.1** – Clarifies the requirement for alternate sites for high availability systems **Section 4.1.l.a** – Added requirement for annual reviews of position sensitivity levels **Section 4.1.1.c** – Exempts active duty USCG and other personnel subject to UCMJ from background check requirements **Section 4.1.4.c-d** – Adds additional separation of duties requirements and restricts the use of administrator accounts **Section 5.2.f** – Limits the number of concurrent connections for FIPS-199 high systems **Section 5.4.2.a** – Limits network monitoring as per the Electronic Communications Act **Section 5.4.3** – Added introduction to clarify ISA requirements **Section 5.4.3.f** – Clarifies the term “security policy” in context **Section 5.4.3.m** – Clarifies that the both AOs must accept risk for interconnected systems that do not require ISAs. **Section 5.4.3.m-n** – Adds stipulations to ISA requirements **Section 5.5** – Updates language in entire section **Section 5.5.3.j** – Assigns the DHS PKI MA responsibility for maintaining Human Subscriber agreements

Version	Date	Description
7.2.1	August 9, 2010	**General Updates** No general updates with this revision. Specific updates are listed below. **Specific Updates** **Section 1.1** – Removes reference to 4300C; updates section to align with policy **Section 1.4.1/3** – Updates Executive Order reference from 12958 to 13526 **Section 1.4.8** – Updates definition of DHS system to align with policy **Section 1.4.17** – Updates the PII section **Section 1.4.18** – Updates SPII section **Section 1.5.3** – Adds requirement for Privacy Officer/PPOC approval for exceptions and waivers pertaining to Privacy Designated Systems **Section 1.6.b/c** – Requires installation and use of digital signatures and certificates **Section 2.1.6.d** – Allows delegation of AO duty to review and approve administrators **Section 2.2.6** – Updates DHS Chief Privacy Officer description **Section 3.7.e** – Adds requirement to include DHS certificate as part of FDCC **Section 3.14** – Updates Privacy and Data Security section **Section 3.14.1** – Updates PII section **Section 3.14.2** – Updates PTA section **Section 3.14.2.e** – Updates impact level requirements for Privacy Sensitive Systems **Section 3.14.3** – Updates PIA section **Section 3.1.4.4** – Updates SORN section **Section 3.14.4.a** – Exempts SORN requirements **Section 3.14.5** – Updates Privacy Sensitive Systems protection requirements **Section 3.14.6.a** – Updates privacy incident reporting requirements **Section 3.14.7** – Updates privacy requirements for e-Auth **Section 3.14.7.e** – Adds PIA requirements for eAuth **Section 4.1.1.e** – Expands U.S. citizenship requirement for access to all DHS systems and networks **Section 4.1.4.b** – Allows delegation of AO duty to review and approve administrators **Section 4.6.2.3.c** – Clarifies prohibited use of SMS **Section 4.8.4.h** – Updates the term “trusted” to “cleared” maintenance personnel **Section 4.12.i** – Updates escort requirements for maintenance or disposal

Version	Date	Description
		Section 4.12.j – Requires disabling of dial up on multifunction devices **Section 5.4.3** – Clarifies definition of Network Connectivity **Section 5.4.3.m/n** – Clarifies requirement for ISA and aligns with policy **Section 5.4.6.j** – Requires DHS email systems to use a common naming convention **Section 5.5.3.g** – Prohibits sharing of personal private keys
7.2.1.1	January 19, 2011	**General Updates** No general updates with this revision. Specific updates are listed below. **Specific Updates** **Section 4.8.1.a** – Changes requirement for screensaver activation from five (5) to fifteen (15) minutes of inactivity.
9.1	July 24, 2012	**General Changes** Style, grammar, and diction edited. Updated control references. Updated links. **Replace** "EOC" and "Emergency Operations Center" with "SOC" and "Security Operations Center" respectively. **Replace** "CSIRC" and **"**Computer Security Incident Response Center" with "SOC" and "Security Operations Center" respectively. **Replace "**certification and accreditation" and "C&A" with "security authorization process". **Replace "**Certifying Official" with "Security Control Assessor**".** **Replace** "ST&E Plan" with "security assessment plan". **Replace** "ST&E" with "security control assessment" **Replace** "system security plan" with "security plan" and "SSP" with "SP". **Specific Updates:** **Section 1:** Updated citations. **Section 1.4.8.1:** Change definition to specify that a GSS has only one ISSO. **Section 1.4.8.2:** Change definition to specify that an MA has only one ISSO. **Section 1.5.1:** Include language requiring waiver submissions to be coordinated with the AO. **Section 1.5.2:** Include language requiring waiver submissions to be coordinated with the AO. **Section 1.5.3:** Clarify language regarding submission of waivers and exceptions for CFO designated systems. **Section 1.5.3.a:** New policy element added to state that the 4300A Policy and Handbook apply to all DHS systems unless a waiver or exception has been granted. **Section 1.6:** Section 1.6, Information Sharing and Electronic Signature was

Version	Date	Description
		divided into two sections – Section 1.6, Electronic Signatures, and Section 1.7, Information Sharing. **Section 1.6.b:** Changed to require use of electronic signatures where practicable. **Section 1.6.d:** Added new policy element, "DHS and Component systems shall be able to verify PIV credentials issued by other Federal agencies." **Section 1.6.e:** Updated control reference. **Section 1.8:** Section 1.8, Threats, was added to the policy. **Section 1.8.5:** Section added defining *supply chain threat* and *supply chain.* **Section 2.1.2:** Add DHS CISO role as primary liaison to Component officials, and to perform periodic compliance reviews for selected systems. **Section 2.13:** Update Component CISO duties and add to implement POA&M process and ensure that external providers who operate information systems meet the same security requirements as the Component. Include language to address the designation of a Deputy CISO by the Component CISO. Add two new responsibilities for Component CISO: Serve as principal advisor on information security matters; Report to the Component CIO on matters relating to the security of Component information Systems. Removed a lower bullet that these made redundant. Added Science and Technology (S&T) to the list of Components that shall have fulltime CISOs. NPPD added to the list of Components having a fulltime CISO. **Section 2.1.4:** Update list of Component ISSM duties and create a POA&M for each known vulnerability. **Section 2.1.5:** Add significantly expanded Risk Executive duties. **Section 2.1.6:** Add significantly expanded Authorizing Official duties. **Section 2.1.6.a:** Clarified language (designation of AOs at Department level). **Section 2.1.6.b:** Clarified language (designation of AOs at Component level). **Section 2.1.8.g:** New policy element added to ensure ISSO responsibility for responding to ICCB change request packages. **Section 2.2.4:** Includes new language stating that the Component CISO reports directly to the Component CIO. **Section 2.2.8:** Add Program Manager responsibility for POA&M content. **Section 2.2.9:** Add expanded System Owner duties. **Section 2.2.10:** Renumber previous version's Section 2.2.10 to be Section 2.2.11 **Section 2.2.10 [New]:** Introduces and describes duties of Common Control Provider. **Section 2.2.11:** Renumbered from previous version's 2.2.10. **Section 3.1.k:** Added policy statement requiring SCAP compliance. **Section 3.18:** Section added containing Cloud Services policy. **Section 3.2.g:** Added new policy element, "Procurements for services and

Version	Date	Description
		products involving facility or system access control shall be in accordance with the DHS guidance regarding HSPD-12 implementation." **Section 3.5.2.c:** Updated language to clarify requirements for backup policy and procedures. **Section 3.5.2.f:** Updated language to require table-top exercises for testing the CP for moderate availability systems. **Section 3.7.f:** Added new policy element, "Components shall monitor USGCB (or DHS-approved USGCB variant) compliance using a NIST-validated Security Content Automation Protocol (SCAP) tool." **Section 3.9:** Add requirement for Components to designate a Common Control Provider. **Section 3.9.w:** Policy element added to require common control catalogs for DHS enterprise services. **Section 3.9.x:** Policy element added to require the development of Enterprise System Security Agreements for enterprise services. **Section 3.10.b:** Policy element language was updated to clarify the function of information system security review and assistance programs. **Section 3.11.3:** Added section, including two policy statements, relative to Security Policy Working Group. **Section 3.14.6.e:** Updated reference title and hyperlink. **Section 3.14.7.e:** Policy element revised to require consultation with a privacy officer to determine if a change requires an updated PTA. **Section 3.14.7.h:** New policy element added to ensure that all new DHS information systems or those undergoing major upgrades shall use or support DHS PIV credentials **Section 3.14:** Language updated for readability. **Section 3.14.4.c:** Added new policy element, "Components shall review and republish SORNs every two (2) years as required by OMB A-130." **Section 3.14.7.f:** Added new policy element, "Existing physical and logical access control systems shall be upgraded to use PIV credentials, in accordance with NIST and DHS guidelines." **Section 3.14.7.g:** Added new policy element, "All new systems under development shall be enabled to use PIV credentials, in accordance with NIST and DHS guidelines, prior to being made operational." **Section 3.17:** Added reference to NIST SP 800-66 for more information on HIPAA. **Section 4.1.1.c:** Includes new language to give Components the option to use background investigations completed by another Federal agency when granting system access to Federal employees. **Section 4.1.1.c:** Changed "Minimum Background Investigation (MBI)" to "Moderate Risk Background Investigation (MBI)." **Section 4.1.1.d:** Includes new language to give Components the option to use background investigations completed by another Federal agency when granting system access to contractor personnel. **Section 4.1.4.d:** Language updated to clarify usage of administrator accounts.

Version	Date	Description
		Section 4.1.5.d: Policy element revised to clarify awareness training records requirements. **Section 4.1.5.e:** Policy element revised to clarify role-based training records requirements. **Section 4.1.5.f:** Language updated to clarify requirements for security awareness training plan. **Section 4.1.5.g:** Policy element revised to require submission of an annual role-based training plan. **Section 4.1.5.j:** Policy element revised to require annual DHS CISO review of role-based training programs. **Section 4.1.5.k:** Policy element revised to require biannual submission of roster of significant information security personnel and to specify the standard information security roles. **Section 4.3.1.b:** Language updated to clarify protection of offsite backup media. **Section 4.3.1.f:** Policy element prohibiting connection of DHS removable media to non-DHS systems. It was already stated in 4.3.1.e. **Section 4.5.4:** Added reference to NIST SP 800-58 for more information on VoIP. **Section 4.9.j:** Language updated to require that Component SOCs report operationally to the respective Component CISO. **Section 4.9.k:** New policy element added, "The DHS EOC shall report operationally to the DHS CISO." **Section 4.9.1 [four.nine.ell]:** Added policy statement requiring the NOC/SOC to be under the direction of a Government employee who shall be present at all times. **Section 4.10:** renumbered Section 4.9.1 **Section 4.10.1.1** renumbered to Section 4.9.1.1 **Section 4.10.1.2** renumbered to Section 4.9.1.2 **Section 4.10.1.3** renumbered to Section 4.9.1.3 **Section 4.10.1.4** renumbered to Section 4.9.1.4 **Section 4.10.1.5** renumbered to Section 4.9.1.5 **Section 4.10.1.6** renumbered to Section 4.9.1.6 **Section 4.10.2** renumbered to Section 4.9.2 **Section 4.10.3** renumbered to Section 4.9.3 **Section 4.11** renumbered to Section 4.10 **Section 4.12** renumbered to Section 4.11 **Section 4.13** renumbered to Section 4.12 **Section 4.9.1.b:** Revised with clarification of reporting means and requirements. **Section 4.9.1.c:** Revised with clarification of reporting means and requirements. **Section 4.10:** Revise list of annual system documentation updates. **Section 4.11.c:** Policy element replaced with new one stating that the policy

Version	Date	Description
		applies "to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS data." **Section 4.11.c:** Policy element was moved to 1.5.3.a. **Section 4.12.d:** Updated control reference. **Section 4.11** **Section 4.10.c:** Updated control reference. **Section 5.1.g:** Policy element added to require use of PIV credentials for logical authentication where available. **Section 5.2.b:** Updated control reference. **Section 5.2.e:** Updated control reference. **Section 5.2.f:** Policy element revised to allow concurrent sessions to one if strong authentication is used. **Section 5.2.g:** New policy element added to ensure preservation of identification and access requirements for all data-at-rest. **Section 5.4.1.a:** Updated control reference. **Section 5.4.4.b:** Updated control reference. **Section 5.4.1.e:** Policy element removed. **Section 5.4.1.f:** Policy element removed. **Section 5.4.6.k:** Added policy statement moved from 5.4.7.b. **Section 5.4.7.b:** Deleted and becomes new policy statement 5.4.6.k. **Section 5.5.2:** Revised to address the two DHS PKIs now functioning: DHS FPKI and DHS Internal NPE PKI. **Section 5.5.3:** Revised to address the two DHS PKIs now functioning: DHS FPKI and DHS Internal NPE PKI. **Section 5.7.e:** Updated control reference. **Section 5.8:** Added new section, including two policy statements, relative to IT supply chain risks and protection against supply chain threats. **Appendix A:** Included new acronyms **Appendix B:** Revised definition of Accreditation Package to reflect new list of documentation. **Appendix C:** Updated references
11.0	January 14, 2014	**General:** Removed all policy statements and language regarding exceptions to policy from the document. **Section 1.5.4:** Revised to transfer responsibility to OCSO for granting access to IT systems by non-U.S. citizens. **Section 1.6:** Revised to align with NARA and OMB requirements and guidance on Electronic Signatures. **Section 3.9.1:** Revised to include new Ongoing Authorization (OA) information. **Section 3.18:** Revised policy on cloud services/FedRAMP **Section 4.6.2 (principally) and throughout:** "PED," "PDA," and "wireless PDA" have been replaced with the words "wireless mobile devices." **Section 5.8:** Revised language regarding supply chain