DHS Sensitive Systems Policy Directive 4300A

Version 8.0

March 14, 2011

This is the implementation of
DHS Management Directive 140-01 Information
Technology System Security, July 31, 2007

DEPARTMENT OF HOMELAND SECURITY

This page intentionally left blank

FOREWORD

The Department of Homeland Security (DHS) 4300 series of information security policy is the official series of publications relating to Departmental standards and guidelines adopted and promulgated under the provisions of 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 INFOSEC@dhs.gov or addressed to:

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

Robert C. West
DHS Chief Information Security Officer

This page intentionally left blank

TABLE OF CONTENTS

1.0 INTRODUCTION

This document articulates the Department of Homeland Security (DHS) Information Security Program policies for sensitive systems. Procedures for implementing these policies are outlined in a companion publication, DHS 4300A *Sensitive Systems Handbook*. The handbook serves as a foundation for Components to develop and implement their information security programs. The baseline security requirements (BLSRs) included in the handbook must be addressed when developing and maintaining information security documents.

1.1 Information Security Program

The DHS Information Security Program provides a baseline of policies, standards, and guidelines for DHS Components. This document provides direction to managers and senior executives for managing and protecting sensitive systems. It also outlines policies relating to management, operational, and technical controls necessary for ensuring confidentiality, integrity, availability, authenticity, and nonrepudiation within the DHS information system infrastructure and operations. 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 and Organizations*.

The policies and direction contained in this document apply to all DHS Components. Information security policies and implementing procedures for National Security Systems are covered in separate publications, *DHS National Security Systems Policy Directive 4300B and DHS 4300B National Security Systems Handbook*. These publications are available on the DHS Chief Information Security Officer (CISO) website.

Policy elements are effective when issued. Any policy elements that have not been implemented within ninety (90) days shall be 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. Whenever the DHS Security Compliance tools, Risk Management System (RMS) and TrustedAgent FISMA (TAF) require updating to reflect policy element changes, tool changes shall be available to the Department within forty-five (45) days of the policy 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.

- Public Law 107-347, E-Government Act of 2002, including Title III, Federal Information Security Management Act (FISMA)
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*
- DHS Management Directive (MD) 140-01, *Information Technology Security Services*
- NIST Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*

1.3 Policy Overview

DHS information security policies delineate the security management structure and foundation to measure progress and compliance. Policies in this document are organized under three areas:

- **Management Controls** – Focus on managing both the system information security controls and system risk. These controls consist of risk mitigation techniques and concerns normally addressed by management.
- **Operational Controls** – Focus on mechanisms primarily implemented and executed by people. These 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** – Focus on security controls executed by information systems. These controls provide automated protection from unauthorized access or misuse. They facilitate detection of security violations, and support security requirements for applications and data.

1.4 Definitions

The following definitions apply to the policies and procedures outlined in this document. Other definitions may be found in the National Information Assurance (IA) Glossary, as well as the Privacy Incident Handling Guidance and the Privacy Compliance documentation.

1.4.1 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.

1.4.2 National Intelligence Information

The following definition is provided in *Public Law 108-458, Intelligence Reform and Terrorism Prevention Act of 2004*, December 17, 2004, “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.”

1.4.3 National Security Information

Information that has been determined, pursuant to Executive Order 13526, *Classified National Security Information*, or any predecessor order, to require protection against unauthorized disclosure.

1.4.4 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.

1.4.5 Sensitive Information

Sensitive information is 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 programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security number; trade secrets; system vulnerability information; pre-solicitation procurement documents, such as statements of work; and 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 shall be 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.

1.4.6 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 Web sites).

1.4.7 Information Technology

The Clinger-Cohen Act 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 within this policy document, is equivalent to the term “IT system.”

1.4.8 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.

1.4.8.1 General Support System

A general support system (GSS) is an interconnected set of information resources under the same direct management control that share common functionality. A GSS normally includes hardware, software, information, applications, communications, data and users. Examples of a GSS include a local area network (LAN), including smart terminals that support a branch office, a Department-wide backbone, a communications network, or a Departmental data processing center including its operating system and utilities.

Note: Security for GSS in use at DHS Headquarters shall be under the oversight of the DHS Office of the Chief Information Officer (OCIO), with support from the DHS Enterprise Operations Center (EOC). All other GSS shall be under the direct oversight of the respective Component CISOs, with support from the appropriate Component Security Operations Center (SOC). All GSS must have an Information Systems Security Officers (ISSO) assigned.

1.4.8.2 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 in them, however, require special management oversight and should be treated as major. 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/Information System Security Manager (ISSM), and must have anISSO assigned.

1.4.9 Component

A DHS Component is any of the entities within DHS, including all DHS offices and independent agencies.

1.4.10 Trust Zone

A Trust Zone consists of a group of people, information resources, data systems, and/or networks subject to a shared security policy (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.

1.4.11 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] OMB Circular A-130

1.4.12 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.

1.4.13 Essential Functions

Functions that enable Federal Executive Branch agencies to provide vital services, exercise civil authority, maintain the safety and well being of the general populace, and sustain the industrial/economic base during an emergency.

1.4.14 Vital Records

Electronic and hardcopy documents, references, records, databases, and information systems needed to support essential functions under the full spectrum of emergencies. Categories of these types of 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, as well as related policy or procedural records.
- *Legal and financial rights* records – 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 (Executive Order [E.O.] 12656).*

1.4.15 Operational Data

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

1.4.16 Federal Information Security Management Act

FISMA requires each agency to develop, document, and implement an agency-wide information security program to provide a high-level of security for the information and information systems that support 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 Federal policies and procedures as may be prescribed by OMB and NIST, or other agencies when appropriate

ii. Minimally acceptable system configuration requirements, as determined by the agency

iii. 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 systems or groups of information systems, as appropriate;

(4) Security awareness to inform personnel, including contractors, others working on behalf of DHS, and other users of information systems that support operations and assets of the Department, of:

a. Information security risks associated with their activities

b. Their responsibilities in complying 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;

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

(7) Procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines promulgated 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 the US-CERT

c. Notifying and consulting with:

i. Law enforcement agencies and relevant Offices of Inspector General

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 for information systems that support the operations and assets of the Department

FISMA requires the Chief Information Officer (CIO) to designate a senior agency information security official who shall develop and maintain a Department-wide information security program as required by the statute. Responsibilities include:

- Developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements
- Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities
- Assisting senior Department officials concerning their responsibilities under the statute
- Ensuring that the Department has trained personnel sufficient to assist the Department in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and
- Ensuring that the Department CIO, in coordination with other senior Department officials, reports annually to the Department head on the effectiveness of the Department information security program, including progress of remedial actions

1.4.17 Personally Identifiable Information

Personally Identifiable Information (PII) is any information that permits the identity of an individual to be directly or indirectly inferred, including any information which 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 employee or contractor to the Department.

1.4.18 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 number (A-number), criminal history information, and medical information. Sensitive PII requires stricter handling guidelines due to the sensitivity of the information.

1.4.19 Privacy Sensitive System

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

1.4.20 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.

1.4.21 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 and Exceptions

1.5.1 Waivers

Components may request waivers to, or exceptions from, any portion of this policy, for up to six (6) months, any time they are unable to fully comply with policy requirements. Requests are made, through the Component's ISSO for the system, to the Component's CISO/ISSM, and then to the DHS CISO. All submitters shall coordinate with the AO prior to submission. If a material weakness is reported in an audit report, and the control weakness is not scheduled to be remediated within twelve (12) months, the Component must submit a waiver request to the DHS CISO. If the material weakness is against a financial system, the Component Chief Financial Officer (CFO) must also approve the waiver request before sending to the DHS *CISO*.

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

1.5.2 Exceptions

Components may request an exception whenever they are unable to bring a system control weakness into compliance or when it requires a permanent exception to DHS policy. Exceptions are generally limited to systems that are unable to comply due to detrimental impact to mission, excessive costs, and/or clearly documented end of platform life for non-essential systems within eighteen (18) months, commercial-off-the-shelf (COTS) products that cannot be configured to support the control requirement. This request is made, through the Component CISO/ISSM, to the DHS CISO. All submitters shall coordinate with the AO prior to submission.

The resulting risk also must be approved and accepted by the Authorizing Official (AO) and by the Component CFO if the system is a financial or mixed financial system.

1.5.3 Waiver or Exception Requests

The Waivers and Exceptions Request Form, located in Attachment B of the DHS 4300A *Sensitive Systems Handbook*, shall be used.

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

Waiver requests shall include the operational justification (document mission impact), risk acceptance, risk mitigation measures, and a POA&M for bringing the system procedures or control weakness into compliance.

Exception requests shall include the operational justification (document mission impact), as well as efforts to mitigate the risk based to include descriptions of counter measures or compensating controls currently in place.

Any waiver or exception requests for CFO Designated Systems must be submitted to and approved by the Component's CFO prior to the DHS CFO's submission to the DHS CISO. Any waiver or exception requests 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.

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

Policy ID	DHS Policy Statements	Relevant Controls
1.5.3.a	Systems without an Authorization to Operate (ATO) when this policy is issued shall comply with all of its policy statements or obtain appropriate waivers and/or exceptions.	PL-1
1.5.3.b	Systems with an ATO when this policy is issued shall comply with all of its policy statements within ninety (90) days or obtain appropriate waivers and/or exceptions. (A new ATO is only required for significant changes.)	PL-1
1.5.3.c	Each waiver or exception request shall include the system name, and system TrustedAgent FISMA (TAF) Inventory ID, operational justification, and risk mitigation.	CM-3
1.5.3.d	Components shall request a waiver whenever they are *temporarily* unable to comply fully with any portion of this policy.	CA-2
1.5.3.e	All waiver requests shall identify the POA&M for bringing the system or program into compliance.	CA-5, PM-4
1.5.3.f	The Component CISO/ISSM shall approve all waiver requests prior to submitting them to the DHS CISO.	CA-6
1.5.3.g	Requests submitted without sufficient information shall be returned for clarification prior to making a decision.	CA-6
1.5.3.h	A waiver shall be issued for six (6) months or less. The DHS CISO reserves the right to issue waivers for longer than six (6) months in exceptional situations. Waivers may be renewed by following the same process as in the initial request.	CA-2
1.5.3.i	The Head of the Component shall approve any waiver request that results in a total waiver time exceeding twelve (12) months before sending it to the DHS CISO. The waiver shall also be reported as a material weakness in the Component’s FISMA report.	---
1.5.3.j	Components shall request an exception whenever they are permanently unable to comply fully with any portion of this policy.	CA-2
1.5.3.k	All approved waivers shall be reported in the Component’s FISMA report.	CA-6
1.5.3.l	The DHS CFO shall approve all requests for waivers and exceptions for financial systems prior to their submission to the DHS CISO.	CA-6
1.5.3.m	The Component’s Privacy Officer or Senior PPOC shall approve all requests for waivers and exceptions for Privacy Sensitive Systems prior to their submission to the DHS CISO.	

1.5.4 U.S. Citizen Exception Requests

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; however at times there is a need to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to appropriate policies are treated separately from standard exceptions and waivers. The approval chain for an exception to the U.S. Citizenship requirement flows through the Component Head, the Office of Security, and the CIO. An electronic form for requesting exceptions to the U.S. Citizenship requirement is published in Attachment J of the *DHS 4300A Sensitive Systems Handbook*.

Policy ID	DHS Policy Statements	Relevant Controls
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	The System Owner shall submit each request for exception to the U.S. Citizenship policy to the Component Head. The Component Head shall obtain concurrence from the DHS Chief Security Officer (CSO) and CIO prior to the approval becoming effective.	PS-3
1.5.4.c	Additional compensating controls shall be maintained for foreign nationals, based on nations lists maintained by the DHS CSO.	PS-3

1.6 Information Sharing and Electronic Signature

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

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

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

- Entering incident information into the DHS EOC 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

Policy ID	DHS Policy Statements	Relevant Controls
1.6.a	For DHS purposes, electronic signatures are preferred to pen and ink or facsimile signatures in all cases, except where pen and ink signatures are required by public law, Executive Order, or other agency requirements.	---
1.6.b	Components are encouraged to use electronic signatures whenever possible.	---
1.6.c	Components shall accept electronic signatures whenever the signature's digital certificate is current, electronically verifiable, and issued by a medium or high assurance DHS Certification Authority (CA) or other medium or high CA under the Federal Bridge Certification Authority (FBCA) or Common Authority.	---
1.6.d	DHS and Component systems shall be able to verify PIV credentials issued by other Federal agencies.	

1.7 Changes to Policy

Procedures and guidance for implementing this policy are outlined in a companion publication, *DHS 4300A Sensitive Systems Handbook* with attachments. 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 policies found in this policy document and of the procedures and guidance found in the *DHS 4300A Sensitive Systems Handbook*, contact the DHS CISO at infosec@dhs.gov.

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

Policy ID	DHS Policy Statements	Relevant Controls
1.7.a	The DHS CISO shall be the authority for interpretation, clarification, and modification of the *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* (inclusive of all appendices and attachments).	PL-1
1.7.b	The DHS CISO shall update the *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* at least annually.	PL-1

2.0 ROLES AND RESPONSIBILITIES

Security is an inherently Governmental responsibility; contractors, others working on behalf of 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 following subsections.

2.1.1 DHS Senior Agency Information Security Officer

Policy ID	DHS Policy Statements	Relevant Controls
2.1.1.a	The DHS CISO shall perform the duties and responsibilities of the DHS Senior Agency Information Security Officer (SAISO).	PL-1, PM-2

2.1.2 DHS Chief Information Security Officer

The DHS CISO shall implement and manage 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 CIO and is the principal advisor for information security matters.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.2.a	The DHS CISO shall implement and manage the DHS-wide Information Security Program.	PL-1, PM-2
2.1.2.b	The DHS CISO will serve as the CIO’s primary liaison with the organization’s authorizing officials, information system owners and ISSOs.	---

The DHS CISO:

Implements and manages the Department-wide Information Security Program and ensures compliance with FISMA, OMB, and other Federal requirements

- Issues Department-wide information security policy, guidance, and architecture requirements for all DHS systems and networks. These policies shall incorporate NIST guidance, as well as all applicable OMB memoranda 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 the DHS for matters relating to information security
- Reviews and approves the tools, techniques, and methodologies planned for use in certifying and accrediting DHS systems, and for reporting and managing systems-level FISMA data. This includes Security Assessment plans, Contingency Plans, and security risk assessments.
- Consults with the DHS 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 for information systems
- Ensures that Department personnel, contractors, and others working on behalf of DHS receive appropriate information security awareness
- Chairs the CISO Council. This Council is comprised of all Component CISOs, and is the Department's sole coordination body for any issues associated with information security policy, management, and operations. Component ISSMs will be invited to CISO Council meetings as required
- Maintains a comprehensive inventory of all GSS and MA in use within the Department
    - Security management for every GSS shall be under the direct oversight of either the DHS CISO (for enterprise systems) or a Component CISO/ISSM (for Component-specific general support systems)
    - 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 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 responsibilities for maintaining a high degree of compliance to Component CISOs and ISSMs, as appropriate
- Reports annually to the Secretary on the effectiveness of the Department information security program, including progress of remedial actions. This report provides the primary basis for the Secretary's annual FISMA report to both OMB and to the United States Congress.

- 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
- Provide operational direction to the DHS 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 that implement FISMA, other laws, and Executive Orders.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.3.a	Component CISOs shall develop and maintain a Component-wide information security program in accordance with the DHS security program.	PL-1, PM-2
2.1.3.b	All Components shall be accountable to the appropriate CISO. Components without a fulltime CISO shall be responsible to the HQ CISO.	---

The following Components shall have a fulltime CISO:

- Customs and Border Protection
- Immigration and Customs Enforcement
- Transportation Security Administration
- United States Secret Service
- United States Coast Guard
- Federal Emergency Management Agency
- United States Citizenship and Immigration Services
- Federal Law Enforcement Training Center
- Headquarters, Department of Homeland Security
- Intelligence and Analysis

Component CISOs:

- Oversee the Component information security program
- Ensure that the Component CIO is kept apprised of all pertinent matters involving the security of information systems

- 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 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 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. Review and approve ISSO appointments
- Ensure that weekly incident reports are submitted to the DHS EOC
- Acknowledge receipt of ISVM messages, report compliance with requirements or notify the granting of waivers
- Manage Component firewall rule sets
- Ensure that Interconnection Security Agreements (ISAs) are maintained for all connections between systems that do not have the same security policy
- Ensure execution of the DHS Logging Strategy detailed in the *DHS 4300A Sensitive Systems Handbook*
- Ensure adherence to the DHS Secure Baseline Configuration Guides (DHS 4300A Sensitive Systems Handbook, Enclosure 1)
- Ensure reporting of vulnerability scanning activities to the DHS EOC as detailed in *Attachment O, Vulnerability Management Program*, of *DHS 4300A Sensitive Systems Handbook*
- 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 address all applicable requirements
- Ensure training and oversight for personnel with significant responsibilities for information security
- Oversee the Security Authorization process for GSSs and MAs in use within the Component
    - Maintain an independent Component-wide Assessment program to ensure a consistent approach to testing of effectiveness of controls

  - Ensure that an appropriate SOC performs an independent network assessment as part of the assessment process for each application that is accredited
  - Ensure that enterprise security tools are utilized

- Exercise oversight over all Component security operations functions, including the Component SOCs

  Ensure that eternal providers who operate information systems on behalf of the Component meet the same security requirements as the Component with an acceptable level of trust in the external service, or else use compensating controls to constrain the nature of information or the process flow, accept a greater degree of risk, or decline the service and reduce functionality

Component CISO qualifications include:

- Possess professional qualifications, including training and experience, required to administer the functions described, including maintaining a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance
- Have information security duties as that official's primary duty
- Participate in the DHS CISO Council, chaired by the DHS CISO
- Head an office with the mission and resources to assist in ensuring Component compliance with this directive and to coordinate, develop, implement, and maintain an organization-wide information security program
- Serve as the Component Risk Executive

2.1.4 Component Information Systems Security Manager

Components that are not required to have a fulltime CISO shall have a fulltime Information Systems Security Manager (ISSM). The ISSM is designated in writing by the Component CIO, with the concurrence of the HQ CISO.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.4.a	Component ISSMs shall serve as the principal interface between the HQ CISO, Component ISSOs and other security practitioners.	---
2.1.4.b	The Component ISSM shall work directly with the HQ 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 HQ CISO are kept apprised of all pertinent matters involving the security of information systems

- 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
- 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
- Periodically test the security of implemented systems
- 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 information system managed at the Component level
- Ensure that weekly incident reports are forwarded to the HQ CISO
- Acknowledge receipt of Information Security Vulnerability Management (ISVM) messages, report compliance with requirements or notify the granting of waivers
- Ensure adherence to the DHS Secure Baseline Configuration Guides (DHS 4300A Sensitive Systems Handbook, Enclosure 1)
- Develop and publish procedures necessary to implement the requirements of DHS information security policy within the appropriate 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 MAs in use within the Component
    - Maintain an independent Component-wide ST&E Program to ensure a consistent approach to testing of effectiveness of controls
    - Ensure that an appropriate SOC performs an independent network assessment as part of the ST&E process for each application that is accredited
    - Ensure that enterprise security tools are utilized

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 Executives – 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 inputs are documented and become part of the security authorization decision. All DHS Risk Executives:

- Ensure that managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is performed as part of an organization-wide process that considers other organizational risks affecting mission/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 authorizing officials 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 authorizing officials and other senior leaders within the organization in order to help these officials consider all types of risks that may 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 and exceptions to DHS policy.

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

Policy ID	DHS Policy Statements	Relevant Controls
2.1.5.a	The DHS CIO shall be the DHS Risk Executive. (The DHS CISO has been designated by the DHS CIO as the Risk Executive.)	PL-1, PM-9
2.1.5.b	Each Component CISO shall be the Risk Executive within his or her Component.	PL-1, PM-9
2.1.5.c	The Risk Executive shall perform their duty in accordance with NIST SP 800-37.	

2.1.6 Authorizing Official

The Authorizing Official (AO) formally assumes responsibility for operating an information system at an acceptable level of risk. He or she shall be a senior management official and a Federal employee or military member. The Authorizing Official will also assign the Security Control Assessor for the system.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.6.a	The DHS CIO shall act as the AO for enterprise information systems or shall designate one in writing.	CA-6

Policy ID	DHS Policy Statements	Relevant Controls
2.1.6.b	The Component CIO shall act as the AO for Component information systems or shall designate one in writing.	CA-6
2.1.6.c	Every system shall have a designated AO. (An AO may be responsible for more than one system.)	CA-6
2.1.6.d	The AO shall review and approve any individual requiring administrator privileges. The AO may delegate this duty to the appropriate system owner or Program Manager.	AC-2
2.1.6.e	The AO shall be responsible for acceptance of resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.	CA-6
2.1.6.f	The AO shall periodically review security status to determine if risk remains acceptable	CA-6
2.1.6.g	The AO shall perform additional duties in accordance with NIST SP 800-37	CA-6

2.1.7 Security Control Assessor

The Security Control Assessor is a senior management official who certifies the results of the security assessment. A Certifying Official is assigned in writing to each information system by an appropriate Component official, typically the Component Head or Component CIO. He or she shall be a Federal employee.

The Security Control Assessor and the team conducting a certification must be impartial, that is, free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system or to the determination of security control effectiveness.

For systems with low impact, a Security Control Assessor and/or certifying team do 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 veracity.

The AO decides the required level of certifier independence based on the criticality and sensitivity of the information system and the ultimate risk to organizational operations, organizational assets, and individuals. The AO determines if the level of certifier independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make credible, risk-based decisions.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.7.a	The Component CISO shall serve as Security Control Assessor when no other person has been officially designated.	CA-2
2.1.7.b	A Security Control Assessor may be responsible for more than one system.	CA-2

Policy ID	DHS Policy Statements	Relevant Controls
2.1.7.c	The Security Control Assessor may take the lead for any or all remedial actions.	CA-7
2.1.7d	The Security Control Assessor provides an assessment of the severity of weaknesses or deficiencies in the information systems, and clarifies they prepare the final security assessment report containing the results and findings from the assessment but not making a risk determination.	CA-7

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 *DHS 4300A Sensitive Systems Handbook, Attachment C – Information Systems Security Officer (ISSO) Designation Letter*.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.8.a	An ISSO shall be designated for every information system and serve as the point of contact (POC) for all security matters related to that system.	PL-1
2.1.8.b	An ISSO shall ensure the implementation and maintenance of security controls in accordance with the Security Plan (SP) and DHS policies.	PL-1
2.1.8.c	An ISSO may be a DHS employee or a contractor.	PL-1
2.1.8.d	An ISSO may be assigned to more than one system.	PL-1
2.1.8.e	ISSO duties shall not be assigned as collateral duties unless approved by the Component CISO.	PL-1
2.1.8.f	The ISSO shall have a clearance greater than or equal to the highest level of information contained on the system. The minimum clearance for an ISSO shall be Secret.	

2.2 Other Roles

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

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 (1) the DHS CIO's assessment of the adequacy and effectiveness of the Department's information security procedures, practices, and FISMA compliance, (2) the results of an annual independent information security program evaluation performed by the DHS Office of the Inspector General (OIG), and (3) the Senior Agency Official for Privacy's (SAOP) annual assessment of the Department's privacy policies, procedures, and practices to the Director of OMB
- Provides information security protections commensurate with the risk and magnitude of the harm resulting 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 senior agency officials within the Department are given 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 the heads of DHS Components are responsible for oversight of the Component information security program, including appointing CIOs. Persons filling this role allocate adequate resources to information systems for information system security.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.2.a	The Under Secretaries of Homeland Security and Heads of Components shall ensure that information systems and their data are sufficiently protected.	PL-1

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.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.3.a	The DHS CIO shall develop and maintain the DHS Information Security Program.	PL-1
2.2.3.b	The DHS CIO designates the DHS CISO.	PL-1

The DHS CIO:

- Oversees the development and maintenance of a Department-wide information security program
- Appoints a DHS employee in writing to serve as the DHS CISO
- Serves as the AO for DHS enterprise information systems. This responsibility may be delegated in writing as appropriate
- 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
- Heads an office with the mission and resources to assist in ensuring Component compliance with the DHS Information Security Program
- 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.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.4.a	The Component CIO shall develop and maintain the Component Information Security Program.	PL-1, PM-1

Component CIOs:

- Establish and oversee their Component information security programs
- Ensure that an AO has been appointed for all Component information systems and serve as the AO for any information system where an AO has not 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 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 issues that may cause public concern or loss of credibility
- Ensure that incidents are reported to the DHS EOC within reporting time requirements as defined in Attachment F, *Incident Response* of the *DHS Sensitive Systems Handbook*

- 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

The following Component CIOs shall appoint a CISO and ensure that the CISO has resources to assist with Component compliance with policy. CISOs shall be DHS employees.

- Customs and Border Protection
- Immigration and Customs Enforcement
- Transportation Security Administration
- United States Secret Service
- United States Coast Guard
- Federal Emergency Management Agency
- United States Citizenship and Immigration Services
- Federal Law Enforcement Training Center

All other Component CIOs:

- Ensure that Component ISSMs have been appointed and 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.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.5.a	DHS information systems that control physical access shall be approved to operate in accordance with this policy document, whether they connect to other DHS information systems or not.	CA-1
2.2.5.b	The DHS CSO shall be the AO for all systems automating or supporting physical access controls or shall appoint an AO for each of those systems.	CA-6

2.2.6 DHS Chief Privacy Officer

The DHS Chief Privacy Officer is the head of the DHS Privacy Office and oversees privacy activities throughout DHS.including creating and ensuring compliance with privacy policy. The DHS Chief Privacy Officer assists the Component Privacy Officers and Privacy Points of Contact (PPOC) with privacy policy compliance at the Component level.

The DHS Chief Privacy Officer implements and manages the DHS Privacy Program, including creating DHS privacy policy and ensuring compliance with privacy policy. The DHS Chief Privacy Officer is responsible for DHS privacy policy and its compliance. The DHS Chief Privacy Officer assists the Component Privacy Officers and PPOC with policy compliance at the Component level.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.6.a	The Chief Privacy Officer shall review program and system Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), and System of Records Notices (SORN), providing approval as appropriate.	PL-1, PL-5

The Chief Privacy Officer, as the senior official:

- Oversees privacy incident management
- Responds to suspected or confirmed privacy incidents or incidents involving PII
- Coordinates with the DHS CIO, DHS CISO, the DHS EOC, and senior management regarding privacy incidents
- Convenes and chairs incident response teams, such as the Privacy Incident Response Team (PIRT) and the Core Management Group (CMG)
- Approves program and system PTAs, PIAs, and SORNs
- Designates Privacy Sensitive Systems based on validated PTAs. Privacy Sensitive Systems are those that maintain PII
- Provides Department-wide annual and refresher privacy training

2.2.7 DHS Chief Financial Officer

The DHS 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.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.7.a	The DHS CFO shall be the AO for all financial systems managed at the DHS level.	CA-6
2.2.7.b	The Component CFO shall be the AO for all financial systems managed by the Component.	CA-6
2.2.7.c	The DHS CFO shall designate the financial systems that fall under the DHS CFO mandated policy statements.	CA-6

Policy ID	DHS Policy Statements	Relevant Controls
2.2.7.d	The DHS CFO shall publish a comprehensive list of designated financial systems during the fourth quarter of every fiscal year. (This list shall be referred to as the CFO Designated Systems List.)	CA-6

All systems on the CFO Designated Systems List are required to conform with 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.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.8.a	Program Managers shall ensure that program POA&Ms are prepared and maintained.	CA-5, PM-4
2.2.8.b	Program Managers shall prioritize security weaknesses for mitigation.	CA-5
2.2.8.c	Program Managers shall provide copies of program POA&Ms to affected System Owners.	CA-5, PM-4
2.2.8.d	Program Managers shall ensure that POA&Ms address the following: ▪ known vulnerabilities in the information system ▪ the security categorization of the information system ▪ the specific weaknesses or deficiencies in the information system security controls ▪ the importance of the identified security control weakness or deficiencies ▪ the Component’s proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls the Component’s rationale for accepting certain weaknesses or deficiencies in the security controls.	CA-5

2.2.9 System Owners

System Owners use information technology 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.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.9.a	System Owners shall ensure that each of their systems is deployed and operated in accordance with this policy document.	PL-1
2.2.9.b	System Owners shall ensure that an ISSO is designated in writing for each information system under their purview.	PL-1
2.2.9.c	There shall be only one System Owner designated for each DHS system.	PL-1
2.2.9.d	The Information System Owner shall information security compliance, development and maintenance of security plans, user security training, notifying officials of the need for security authorization and need to resource.	CA-2
2.2.9.e	System Owners shall ensure development of a POA&M to address weaknesses and deficiencies in the information system and its environment of operation which remain after Security Authorization.	CA-2

2.2.10 Common Control Provider

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

2.2.10.a	The Common Control Provider shall document all common controls and submit them to the AO and DHS CISO.	PM-1
2.2.10.b	The Common Control Provider ensures that required assessments of common controls are carried out by qualified assessors with the appropriate level of independence.	PM-1
2.2.10.c	The Common Control Provider documents assessment findings in a security assessment report.	PM-1
2.2.10.d	The Common Control Provider ensures that POA&Ms are developed for all controls having weaknesses or deficiencies.	PM-4
2.2.10.e	The Common Control Provider shall make available security plans, Security Assessment Reports (SARs), and POA&Ms for common controls to information system owners inheriting those controls after the information is reviewed and approved by a senior official.	PM-1, PM-4

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 shall follow the appropriate set(s) of rules of behavior.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.11.a	DHS users shall follow prescribed rules of behavior.	PL-4

3.0 MANAGEMENT POLICIES

3.1 Basic Requirements

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

Component CISOs/ISSMs shall submit all security reports concerning DHS systems to the Component senior official or designated representative. Component CISOs/ISSMs shall interpret and manage DHS security policies and procedures to meet Federal, Departmental, and Component requirements. They shall also answer data queries from the DHS CISO and develop and manage information security guidance and procedures unique to Component requirements.

ISSOs 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.

Policy ID	DHS Policy Statements	Relevant Controls
3.1.a	Every DHS computing resource (e.g., desktops, laptops, servers, portable electronic devices) shall be individually accounted for as part of a recognized information system.	CM-8
3.1.b	The Component CIO, in cooperation with each Component senior official, shall be responsible for ensuring that every DHS computing resource is identified as an information system or as a part of an information system (major application or general support system).	CM-8
3.1.c	The System Owner or designee shall develop and maintain an SP for each information system. Component AOs shall review and approve SPs.	PL-2
3.1.d	An ISSO shall be designated for every information system and serve as the point of contact (POC) for all security matters related to that system.	PL-1
3.1.e	Component Information Security Programs shall be structured to support DHS and applicable FISMA, OMB, and other Federal requirements.	PL-1
3.1.f	Information security reports regarding DHS systems shall be submitted to the Component senior official or designated representative.	---
3.1.g	Component CISOs/ISSMs shall ensure that their information systems comply with the DHS Enterprise Architecture (EA) Technical Reference model (TRM) and Security Architecture (SA) or maintain a waiver, approved by the DHS CIO/CISO.	PL-1
3.1.h	The DHS CISO shall issue Department-wide information security policy, guidance, and architecture requirements for all DHS systems.	CM-2, CM-6
3.1.i	Component CISOs shall implement DHS information security policies, procedures, and control techniques to address all applicable requirements.	PL-1

Policy ID	DHS Policy Statements	Relevant Controls
3.1.j	Component CISOs shall develop and manage information security guidance and procedures unique to Component requirements.	PL-1

3.2 Capital Planning and Investment Control

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. Directive 102-01, Acquisition Management Directive and MD 4200.1, IT Capital Planning and Investment Control (CPIC), and Portfolio Management provide additional information on these requirements.

Policy ID	DHS Policy Statements	Relevant Controls
3.2.a	System Owners shall include information security requirements in their CPIC business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP) for each DHS system.	PM-3, PM-11, SA-1
3.2.b	System Owners or AOs shall ensure that information security requirements and POA&Ms are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.	PM-3, PM-4, SA-2
3.2.c	Component IRBs/ARBs shall not approve any capital investment in which the information security requirements are not adequately defined and funded.	PM-3, SA-2
3.2.d	The DHS CISO shall perform security reviews for planned information system acquisitions over $2.5 million and additional selected cases.	SA-1
3.2.e	Components shall ensure that information security requirements as described within this policy document are included in the acquisition of all DHS systems and services used to input, process, store, display, or transmit sensitive information.	SA-4
3.2.f	Procurement authorities throughout the Department shall ensure that Homeland Security Acquisition Regulation (HSAR) provisions are fully enforced.	SA-1, SA-4
3.2.g	Procurements for services and products involving facility or system access control shall be in accordance with the DHS guidance regarding HSPD-12 implementation.	

3.3 Contractors and Outsourced Operations

Policy ID	DHS Policy Statements	Relevant Controls
3.3.a	All statements of work and contract vehicles shall identify and document the specific security requirements for information system services and operations required of the contractor.	SA-4
3.3.b	Contractor information system services and operations shall adhere to all applicable DHS information security policies.	SA-9
3.3.c	Requirements shall address how sensitive information is to be handled and protected at contractor sites, including any information stored, processed, or transmitted using contractor information systems. Requirements shall also include requirements for personnel background investigations and clearances, and facility security.	SA-9
3.3.d	Statements of work and contracts shall include a provision stating that, upon the end of the contract, the contractor shall return all information and information resources provided during the life of the contract and certify that all DHS information has been purged from any contractor-owned system used to process DHS information.	SA-4
3.3.e	Components shall conduct reviews to ensure that the information security requirements are included within the contract language and are implemented and enforced.	SA-1
3.3.f	Security deficiencies in any outsourced operation shall require creation of a program-level POA&M.	SA-9, PM-4

3.4 Performance Measures and Metrics

Policy ID	DHS Policy Statements	Relevant Controls
3.4.a	The DHS CISO shall define performance measures to evaluate the effectiveness of the DHS information security program.	---
3.4.b	Components shall provide OMB FISMA data at least monthly to the DHS Compliance Officer.	---
3.4.c	The DHS CISO shall report annually to the Secretary on the effectiveness of the DHS information security program, including the progress of remedial actions.	---
3.4.d	Components shall utilize the automated tool directed for use by the DHS CISO for Performance Plan reporting.	---

Policy ID	DHS Policy Statements	Relevant Controls
3.4.e	The DHS CISO shall collect OMB FISMA data from Components at least quarterly and provide FISMA reports to OMB.	---

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), which is part of the Contingency, is essential in the identification of critical DHS assets. Once critical systems are identified, continuity planning shall address the following two complementary but different elements:

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

3.5.1 Continuity of Operations Planning

Policy ID	DHS Policy Statements	Relevant Controls
3.5.1.a	When available, a DHS-wide process for continuity planning shall be used in order to ensure continuity of operations under all circumstances.	CP-2
3.5.1.b	Components shall develop, test, implement, and maintain comprehensive Continuity of Operations Plans (COOP) to ensure the continuity and recovery of essential DHS functionality.	CP-2, CP-4
3.5.1.c	All CISOs/ISSMs shall ensure that all COOPs under their purview are tested and exercised annually.	CP-4
3.5.1.d	All CFO Designated Systems requiring high availability shall be identified in COOP plans and exercises.	CP-1
3.5.1.e	All personnel involved in COOP efforts shall be identified and trained in the procedures and logistics of COOP development and implementation.	AT-3, CP-3
3.5.1.f	To ensure that accounts can be created in the absence of the usual account approval authority, systems that are part of the Critical DHS Assets Program shall have provisions to allow a Component CISO/ISSM or Component CIO to approve new user accounts as part of a COOP scenario.	AC-2
3.5.1.g	Each Component shall compile and maintain a list of mission-critical information systems in support of COOP.	CM-8, CP-1
3.5.1.h	The DHS and Component CISOs/ISSMs shall ensure preparation and maintenance of plans and procedures to provide continuity of operations for information systems.	CP-1

Policy ID	DHS Policy Statements	Relevant Controls
3.5.1.i	DHS information systems that are part of the DHS Continuity Planning for Critical DHS Assets Program shall be provided requirements for system-level contingency planning by a Component Contingency Planning Program Office or by a DHS Contingency Planning Program Office.	---

3.5.2 Contingency Planning

Policy ID	DHS Policy Statements	Relevant Controls
3.5.2.a	The DHS CIO shall provide guidance, direction, and authority for a standard DHS-wide process for contingency planning for all DHS Components.	CP-1
3.5.2.b	System Owners shall develop and document information system Contingency Plans (CPs) for their programs, manage plan changes, and distribute copies of the plan to key contingency personnel. Component CIOs shall review and approve Component-level information system CPs.	CP-1, CP-2
3.5.2.c	Components shall ensure implementation of backup policy and procedures for every Component information system.	CP-9
3.5.2.d	The DHS CIO shall ensure that each system has contingency capabilities commensurate with the **availability** security objective. The minimum contingency capabilities for each impact level follow: **High** – System functions and information have a high priority for recovery after a short period of loss. **Moderate** – System functions and information have a moderate priority for recovery after a moderate period of loss. **Low** – System functions and information have a low priority for recovery after prolonged loss.	CP-1
3.5.2.e	CPs shall be developed and maintained by all DHS Components in accordance with the requirements for the FIPS 199 potential impact level for the **availability** security objective. These plans shall be based on three essential phases: Activation/Notification, Recovery, and Reconstitution. Components shall review the CP for the information system at least annually and revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	CP-1, CP-2
3.5.2.f	The DHS CIO shall ensure that CP testing is performed in accordance with the **availability** security objective. The minimum contingency testing for each impact level follows: **High** – System recovery roles, responsibilities, procedures, and logistics in the CP shall be used to recover from a simulated contingency event at the alternate processing site within a year prior to accreditation. The system recovery procedures in the CP shall be used to simulate system recovery in a test facility at least annually.	CP-4, CP-7

Policy ID	DHS Policy Statements	Relevant Controls
	Moderate – The CP shall be tested at least annually by reviewing and coordinating with organizational elements responsible for plans within the CP. This is achieved by performing a walk-through/tabletop exercise. **Low** – CP contact information shall be verified at least annually.	
3.5.2.g	The DHS CIO shall ensure that contingency training is performed in accordance with the **availability** security objective. The minimum contingency planning for each impact level follows: **High** – All personnel involved in contingency planning efforts shall be identified and trained in their contingency planning and implementation roles, responsibilities, procedures, and logistics. This training shall incorporate simulated events. Refresher training shall be provided at least annually. **Moderate** – All system personnel involved in contingency planning efforts shall be trained. Refresher training shall be provided at least annually. **Low** – There is no training requirement.	CP-3
3.5.2.h	Components shall coordinate as appropriate CP testing and/or exercises with COOP related plans for systems with moderate and high availability FIPS-199 categorization.	CP-4

3.6 System Engineering Life Cycle

Directive 102-01, Acquisition Management Directive, Appendix B, contains the DHS Systems Engineering Life Cycle (SELC).

Policy ID	DHS Policy Statements	Relevant Controls
3.6.a	Components shall ensure that system security is integrated into all phases of the Systems Engineering Life Cycle (SELC).	SA-3
3.6.b	Components shall ensure that security requirements for sensitive information systems are incorporated into life-cycle documentation.	SA-3
3.6.c	The Program Manager shall review, approve, and sign all custom-developed code prior to deployment into production environments. The Program Manager may delegate this authority to another DHS employee in writing. This authority shall not be delegated to contractor personnel.	RA-5

3.7 Configuration Management

Configuration management (CM) relates to managing the configuration of all hardware and software elements within information systems and networks. CM within DHS consists of a multi-layered structure – policy, procedures, processes, and compliance monitoring. Each Component shall utilize appropriate levels of configuration management.

CM applies to all systems, subsystems, and components of the DHS infrastructure, thereby ensuing 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 are 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

DHS Sensitive Systems Handbook, Enclosure 1, includes the DHS Secure Baseline Configuration Guides.

Policy ID	DHS Policy Statements	Relevant Controls
3.7.a	Components shall develop and maintain a configuration management plan (CMP) for each information system as part of its SP. All DHS systems shall be under the oversight of a Configuration Management responsible officer.	CM-1, CM-9
3.7.b	Components shall establish, implement, and enforce configuration management controls on all information systems and networks and address significant deficiencies as part of a POA&M.	CA-5, CM-3, PM-4
3.7.c	Information security patches shall be installed in accordance with configuration management plans and within the timeframe or direction stated within the Information Security Vulnerability Management (ISVM) message published by the DHS EOC.	SI-2
3.7.d	System Owners shall document the initial system configuration in detail and control all subsequent changes in accordance with the configuration management process.	CM-2, CM-3, CM-9
3.7.e	Workstations shall be configured in accordance with DHS guidance on the U.S Government Configuration Baseline (USGCB) (formerly known as the Federal Desktop Core Configuration [FDCC]). Configuration shall include installation of the DHS Common Policy Object identifier (OID), Common Policy Framework Root CA certificate, and the DHS Principal CA certificate.	CM-2, CM-6, CM-9
3.7.f	Components shall monitor USGCB (or DHS-approved USGCB variant) compliance using a NIST-validated Security Content Automation Protocol (SCAP) tool.	

Policy ID	DHS Policy Statements	Relevant Controls
3.7.g	The System Owner shall request an exception for information systems that use operating systems or applications that are not hardened or do not follow configuration guidance identified in DHS Sensitive Systems Handbook, Enclosure 1, DHS Secure Baseline Configuration Guides. Requests shall include a proposed alternative secure configuration.	CM-2, CM-6
3.7.h	Components shall ensure that CM processes under their purview include and consider the results of a security impact analysis when considering proposed changes.	CM-4

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.

Policy ID	DHS Policy Statements	Relevant Controls
3.8.a	Components shall establish a risk management program in accordance with NIST SP 800-30, *Risk Management Guide for Information Technology Systems* and other applicable Federal guidelines.	RA-1
3.8.b	Component CISOs/ISSMs shall ensure that a risk assessment is conducted whenever high impact weaknesses are identified, or every three (3) years or whenever modifications are made to sensitive information systems, or to their physical environments, interfaces, or user community. The risk assessment shall consider the effects of the modifications on the operational risk profile of the information system. SPs shall be updated and re-certification conducted if warranted by the results of the risk assessment.	RA-3
3.8.c	Component CISOs/ISSMs shall establish an independent Component-wide Security Authorization program to ensure a consistent approach to testing the effectiveness of controls.	RA-1
3.8.d	Risk Executives shall review recommendations for risk determinations and risk acceptability and may recommend changes to the AO and appropriate CIO.	RA-3
3.8.e	Component SOCs shall deploy a Component-wide network scanning program.	RA-5
3.8.f	Special rules apply to CFO Designated Systems. See Section 3.15 for additional information.	---

3.9 Security Authoziation and Security Assessments

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

The DHS *Security Authorization Process Guide* describes detailed processes governing *Security Authorization Process* and system risk assessment.

Detailed information for creating and managing POA&Ms is published in DHS 4300A *Sensitive Systems Handbook, Attachment H – Plan of Action and Milestones (POA&M) Process Guide*.

Policy ID	DHS Policy Statements	Relevant Controls
3.9.a	Components shall assign an impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability) for each DHS information system. Components shall apply NIST SP 800-53 controls as tailored in the DHS 4300A, *Sensitive Systems Handbook, Attachment M* specific to the security objective at the determined impact level.	PM-10, RA-2
3.9.b	Components shall implement NIST SP 800-53 security controls, using the FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems* methodology, based on the FIPS 199 impact level established for each separate security objective (confidentiality, integrity, availability).	---
3.9.c	Recommend that Components pursue type *Security Authorization Process* 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 Process* shall consist of a master *Security Authorization Process* package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites.	---
3.9.d	The AO for a system shall be identified in TrustedAgent FISMA. The Component CIO shall serve as the AO whenever the System Owner or an appropriate program official has not been named as the AO.	---
3.9.e	Component CISOs shall ensure that all information systems are formally assessed through a comprehensive evaluation of their management, operational, and technical security controls.	CA-2, PM-10
3.9.f	The assessment, made as part of and in support of the accreditation process, shall determine the extent to which a particular design and implementation plan meets the DHS required set of security controls.	PM-10
3.9.g	Component CISOs/ISSMs shall ensure that a risk assessment is conducted whenever any modifications are made to sensitive information systems, networks, or to their physical environments, interfaces, or user community. SPs shall be updated and re-authorized conducted if warranted.	PM-9, RA-3

Policy ID	DHS Policy Statements	Relevant Controls
3.9.h	Components shall accredit systems at initial operating capability and every three (3) years thereafter, or whenever a major change occurs, whichever occurs first. An ATO of six (6) months or less shall receive an ATO accreditation period waiver from the DHS CISO before submission to the AO for a final accreditation decision.	CA-6, PM-10
3.9.i	AOs may grant an Interim Authorization to Operate (IATO) for systems that are undergoing development testing or are in a prototype phase of development. A system shall be assessed and authorized in an ATO letter prior to passing the Key Decision Point 3 milestone in the SELC. IATOs shall not be used for operational systems. The AO may grant an IATO for a maximum period of 6 (six) months and may grant 1 (one) 6 (six) month extension. Systems under an IATO shall not process sensitive information but may attach to system networks for testing.	PL-1, PM-10
3.9.j	If the system is not fully accredited and has not received a full ATO by the end of the second and final IATO, the system shall not be deployed as an operational system.	PL-1, PM-10
3.9.k	As a result of Office of Inspector General (OIG) auditing experience, Components shall request concurrence from the DHS CISO for all accreditations for 6 (six) months or less.	---
3.9.l	The DHS CISO shall specify tools, techniques, and methodologies used to certify and accredit DHS information systems, report and manage FISMA data, and document and maintain POA&Ms.	CA-1, PM-4
3.9.m	Currently, all DHS systems shall be accredited using the automated tools, TAF and RMS, which have been approved by the DHS CISO.	CA-1, CA-2, PM-10
3.9.n	The DHS CISO shall maintain a repository for all *Security Authorization Process* documentation and modifications.	CA-1
3.9.o	Component CISOs shall establish processes to ensure consistent *Security Authorization Process* processing across all Component systems.	CA-1, PM-10
3.9.p	System Owners shall use the POA&M process to manage vulnerabilities, correct deficiencies in security controls, and remediate weaknesses in SPs.	CA-5, PM-4
3.9.q	The AO shall formally assume responsibility for operating an information system at an acceptable level of risk. System operation with sensitive information is prohibited without an ATO.	CA-6, PM-10
3.9.r	ATOs shall only be provided for systems that fully comply with policy or have been granted appropriate exceptions or waivers.	CA-6, PM-10

Policy ID	DHS Policy Statements	Relevant Controls
3.9.s	Artifacts in support of *new* ATOs shall not be older than 13 months. Older artifacts remain valid during the life of a current ATO.	---
3.9.t	The DHS CIO may revoke any ATO of any DHS information system.	CA-6
3.9.u	The Component CIO may revoke the ATO of any Component-level information system.	CA-6
3.9.v	Components shall assign a common control provider to share controls between systems (e.g., at hosting centers). The authorization package of those common controls must be shared with those operating under them.	

3.10 Information Security Review and Assistance

Policy ID	DHS Policy Statements	Relevant Controls
3.10.a	Components shall submit their information security policies to the DHS CISO for review.	PL-1
3.10.b	Components shall establish an information system security review and assistance program within their respective security organization in order to provide System Owners with expert review of programs, assist in identifying deficiencies, and provide recommendations for bringing systems into compliance.	CA-7, PL-1, PM-10
3.10.c	Components shall conduct their reviews in accordance with FIPS 200/NIST SP 800-53, for specification of security controls. NIST SP 800-53A shall be used for assessing the effectiveness of security controls and for quarterly and annual FISMA reporting.	CA-7, PL-1
3.10.d	The DHS CISO shall conduct information security review and assistance visits across the Department in order to monitor the effectiveness of Component security programs.	CA-2

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 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 within all enterprise and Component information security programs.

Policy ID	DHS Policy Statements	Relevant Controls
3.11.1.a	Component CISOs shall actively participate in the CISO Council.	PL-1, PM-11
3.11.1.b	Members shall ensure that the DHS CISO is kept apprised of all pertinent matters involving the security of information systems.	PL-1, PM-11
3.11.1.c	Members shall ensure that security-related decisions and information, including updates to the 4300 series of security publications, are distributed to the ISSOs and other appropriate persons.	PL-1, PM-11

Note: Periodically, the CISO Council shall 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.

Policy ID	DHS Policy Statements	Relevant Controls
3.11.2.a	Components shall appoint a representative to the DHS Information Security Training Working Group.	---
3.11.2.b	Members shall actively participate in the DHS Information Security Training Working Group.	---
3.11.2.c	Components shall abide by the security training requirements listed in the Information Security Awareness, Training, and Education section of this policy.	---

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 and violations occur and for holding personnel accountable for intentional transgressions. Each Component must determine how to best address each individual case.

Policy ID	DHS Policy Statements	Relevant Controls
3.12.a	Information security-related violations are addressed in the *Standards of Ethical Conduct for Employees of the Executive Branch* and DHS employees may be subject to disciplinary action for failure to comply with DHS security policy, whether or not the failure results in criminal prosecution.	PS-8
3.12.b	Non-DHS Federal employees, contractors, or others working on behalf of DHS who fail to comply with Department security policies are subject to having their access to DHS systems and facilities terminated, whether or not the failure results in criminal prosecution.	PS-8
3.12.c	Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions.	PS-8

3.13 Required Reporting

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

Policy ID	DHS Policy Statements	Relevant Controls
3.13.a	Components shall collect and submit quarterly and annual information security program status data as required by FISMA.	CA-2
3.13.b	Components shall utilize the automated tool approved for use by the DHS CISO.	CA-2

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 Department information. The DHS Chief Privacy Officer has exclusive jurisdiction over the development of policy relating to personally identifiable information (PII). Questions concerning privacy-related policy should be directed to the Component Privacy Office or PPOC. If the Component does not have a Privacy Office or PPOC, then please contact the DHS Privacy Office (privacy@dhs.gov; 703-235-0780) or refer to the DHS Chief Privacy Officer web page for additional information.

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 any information which is linked or linkable to that individual regardless of whether or not the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

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 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.*

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 Assessments – For Privacy Sensitive Systems, the confidentiality security objective shall be 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 data removed from any accredited system where the process is not covered by the SP and computer-readable data extracts are stored on hard drives, including desk top and laptop computers, floppy disks, compact discs (CDs), digital video disks (DVDs), USB drives, memory cards, and any other media that may be read or copied electronically.
- 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 the DHS Policy.

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 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 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 system development lifecycle 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 0470.2 defines the PTA requirements.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.2.a	A PTA shall be conducted as part of new information system development or whenever an existing system is significantly modified. PTA artifacts expire after three (3) years and a new PTA must be submitted.	PL-5
3.14.2.b	A PTA shall be conducted whenever an information system undergoes security authorization.	---
3.14.2.c	The DHS Chief Privacy Officer shall evaluate the PTA and determine if it is a Privacy Sensitive System and if the system requires a PIA and SORN.	PL-5
3.14.2.d	Information systems shall not be designated operational until the DHS Privacy Office approves the PTA.	PL-5
3.14.2.e	For Privacy Sensitive Systems, the **confidentiality** security objective shall be assigned an impact level of moderate or higher.	RA-2

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 0470.1, and the *Official DHS Privacy Impact Assessment Guidance* discuss the requirements for conducting PIAs at DHS.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.3.a	PIAs are required (as determined by the PTA) as part of new information system development or whenever an existing system is significantly modified.	PL-5
3.14.3.b	Information systems that the DHS Privacy Office has determined require a PIA (as determined by the PTA) shall not be designated operational until the DHS Privacy Office approves the PIA for that system.	PL-5

3.14.4 System of Records 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" 5 U.S.C.§552a (a)(5). 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 an 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. The Office of Management and Budget, specifically *Privacy Act Implementation, Guidelines and Responsibilities,* July 9, 1975, and *Circular A-130* including *Appendix I*, DHS MD 0470.2, and *Official DHS Guidance on System of Records and System of Records Notices* are the benchmark references when developing SORNs.

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.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.4.a	A SORN is required when PII is maintained by a Federal agency in a system of records where information about an individual is retrieved by a unique personal identifier.	---
3.14.4.b	Information systems containing PII shall not be designated operational until a SORN has been published in the Federal Register for thirty (30) days.	CA-6
3.14.4.c	Components shall review and republish SORNs every two (2) years as required by OMB A-130.	

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 as well as media within mobile devices (i.e., laptop hard drive). 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*:
- *DHS* 4300 A, Sensitive System Handbook, Attachment S, *Compliance Framework for Privacy Sensitive Systems*; and
- *DHS Policy and Procedures for 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.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.5.a	PII and Sensitive PII removed from a DHS facility on removable media, such as CDs, DVDs, laptops, PDAs, shall be encrypted, unless the information is being sent to the individual as part of a Privacy Act or Freedom of Information Act (FOIA) request.	MP-5 SC-13
3.14.5.b	If PII and Sensitive PII can be physically removed from an information system (e.g., printouts, CDs), the Security Plan (SP) shall document the specific procedures, training, and accountability measures in place to ensure remote use of the data does not bypass the protections provided by the encryption.	MP-5
3.14.5.c	Systems that, as part of routine business, remove Sensitive PII in the form of a Computer-Readable Extract (CRE), e.g., routine system-to-system transmissions of data (routine CREs) shall address associated risks in the SP.	MP-5
3.14.5.d	Sensitive PII contained within a non-routine or ad hoc CRE (e.g., CREs not included within the boundaries of a source system's security plan) shall not be removed, physically or otherwise, from a DHS facility without written authorization from the Data Owner responsible for ensuring that the disclosure of the CRE data is lawful and in compliance with this and applicable DHS privacy and security policies.	---
3.14.5.e	All ad hoc CREs must be documented, tracked, and validated every ninety (90) days after their creation to ensure that their continued authorized use is still required or that they have been appropriately destroyed or erased.	---

Policy ID	DHS Policy Statements	Relevant Controls
3.14.5.f	Ad hoc CREs shall be destroyed or erased within ninety (90) days unless the information included in the extracts is required beyond that period. Permanent erasure of the extracts or the need for continued use of the data shall be documented by the Data Owner and audited periodically by the Component Privacy Officer or PPOC.	---

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 in OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007 (M-07-16). Through close collaboration, the DHS Chief Privacy Officer, the DHS CIO, the DHS CISO, the DHS EOC, 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.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.6.a	Any Component discovering a suspected or confirmed privacy incident shall coordinate with the Component Privacy Officer or PPOC and Component CISO/ISSM to evaluate and subsequently report the incident to the DHS EOC immediately upon discovery. The DHS EOC will then transmit the report to the US-CERT within one (1) hour.	IR-4
3.14.6.b	The Component Privacy Officer or PPOC, in cooperation with the Component CISO/ISSM, shall jointly evaluate the incident, but the Component CISO/ISSM is responsible for reporting the incident to the Component SOC/ Computer Security Incident Response Capability (CSIRC) (or directly to the DHS EOC/CSIRC if the Component does not have its own SOC/CSIRC).	IR-4
3.14.6.c	For Components without Privacy Officers or PPOCs, the Component CISO/ISSM shall report *all* types of privacy incidents, whether or not they involve information resources. This unitary reporting process shall remain in effect until each Component has a Privacy Officer or PPOC who can fulfill the reporting duties.	IR-6
3.14.6.d	DHS personnel shall also report suspected or confirmed privacy incidents or incidents involving PII to their Program Manager immediately upon discovery/detection, regardless of the manner in which it might have occurred.	IR-6
3.14.6.e	Components shall follow the *DHS Privacy Incident Handling Guide*.	---

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*

Policy ID	DHS Policy Statements	Relevant Controls
3.14.7.a	For systems that allow online transactions, Components shall determine whether e-authentication requirements apply.	IA-2
3.14.7.b	Components shall determine the appropriate assurance level for e-authentication by following the steps described in OMB M-04-04, *E-Authentication Guidance for Federal Agencies*.	IA-2
3.14.7.c	Components shall implement the technical requirements described in NIST SP 800-63, *Electronic Authentication Guideline*, at the appropriate assurance level for those systems with e-authentication requirements.	IA-2
3.14.7.d	Components shall ensure that each SP reflects the e-authentication status of the respective system.	IA-2, PL-2
3.14.7.e	Programs considering the use of e-authentication are required to conduct a PTA to initiate the review of privacy risks and how they will be mitigated.	PL-5
3.14.7.f	Existing physical and logical access control systems shall be upgraded to use PIV credentials, in accordance with NIST and DHS guidelines.	
3.14.7.g	All new systems under development shall be enabled to use PIV credentials, in accordance with NIST and DHS guidelines, prior to being made operational.	

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 OMB Circular A-123, *Management's Responsibility for Internal Control (A-123)*, Appendix A. The requirements contained in OMB Circular A-123 have been mapped to the NIST SP 800-53 controls and documented in DHS 4300A Attachment R. These requirements are in addition to the other security requirements established in this document and other CFO developed financial system Line of Business requirements. *Wherever* *there is a conflict between this and other sections of this policy regarding requirements for CFO Designated Systems, this section takes precedence.*

These additional requirements provide a strengthened assessment process and form the basis for management's assurance on the 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.

Policy ID	DHS Policy Statements	Relevant Controls
3.15.a	System owners are responsible for ensuring that security assessments of key security controls (i.e., Security Assessment and Security Assessment Report [SAR]) for CFO Designated Systems are completed annually in TAF. This includes updating the ST&E & SAR annually.	CA-2, CA-7
3.15.b	The DHS CFO shall designate the systems that must comply with additional internal controls and the Office of the CFO shall review and publish this list annually.	CA-2
3.15.c	Component CISOs/ISSMs shall ensure that vulnerability assessments and verification of critical patch installations are conducted on all CFO Designated Systems. Vulnerability assessment shall be performed at least annually.	RA-5
3.15.d	All CFO Designated Systems shall be assigned a minimum impact level of "**moderate**" for confidentiality, integrity, and availability. If warranted by a risk based assessment, the integrity objective shall be elevated to "high."	RA-2
3.15.e	All Component security accreditations for CFO Designated Systems shall be approved and signed by the Component CFO.	CA-6
3.15.f	System Owners shall ensure that Contingency plans are created for *all* CFO Designated Systems requiring moderate availability and Disaster Recovery plans are created for *all* CFO Designated Systems requiring high availability and that each plan is tested annually.	CP-2, CP-4
3.15.g	Component CISOs/ISSMs shall ensure that weekly incident response tracking is performed for all of their respective CFO Designated Systems.	IR-5
3.15.h	Component CISOs/ISSMs shall ensure that incidents related to their respective CFO Designated Systems are reported to the Component CFO.	IR-4, IR-6
3.15.i	The SP shall be updated for CFO Designated Systems at least annually. Key controls prescribed in Attachment R, *Compliance Framework for CFO Designated Systems* shall be identified in the SP.	PL-2

Policy ID	DHS Policy Statements	Relevant Controls
3.15.j	Component CISOs/ISSMs must request a waiver or exception from the DHS CISO if a key control weakness is identified for a CFO Designated System and not remediated within twelve (12) months.	CA-5, CA-7
3.15.k	Component CFOs shall ensure that a fulltime dedicated ISSO is assigned to each CFO Designated System. CFO Designated System ISSOs may be assigned to more than one CFO Designated System.	---
3.15.l	CFO Designated System ATOs shall be rescinded if Components fail to comply with testing and reporting requirements established within this policy.	CA-1, CA-6
3.15.m	Component CFOs shall work with their Component CISOs/ISSMs to approve any major system changes to CFO Designated Systems identified in the DHS inventory.	CA-1, CM-8

3.16 Social Media

Social Media hosts are public, content sharing Web sites 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) will publish Terms of Service (TOS) and guidelines for posting to these sites. In some cases the Department will develop its own and in other cases 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 TIC.

Policy ID	DHS Policy Statements	Relevant Controls
3.16.a	Only OPA designated content managers (Department level and Component level) may post content, and only those individuals designated by OPA for this purpose shall be granted access on a continuing basis.	SA-6
3.16.b	Posted content shall be in keeping with the Department’s Terms of Service (TOS) and guidelines for a given social media host (e.g., YouTube, Twitter). This condition is also met if the Department endorses another appropriate Federal agency’s guidance or TOS (e.g., GSA, OPM). Under no circumstances shall sensitive information be posted to social media sites.	---
3.16.c	Content shall not be posted to any social media site for which the Department has not approved and published final posting guidelines *and* TOS.	SA-6
3.16.d	Content managers shall review and understand the appropriate Department-level TOS for the appropriate social media host.	---

Policy ID	DHS Policy Statements	Relevant Controls
3.16.e	Content managers shall make a risk decision prior to posting any information and shall recognize that social medial hosts are not DHS information systems and therefore subject only to the DHS TOS and not to DHS policy. Once released, information is no longer under DHS control.	---

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) – Section 5.4.4
- Host Configuration and Hardening – Section 4.8.4
- Enterprise Operations Center (EOC) and Network Operations Center (NOC) – Section 4.9
- Two-Factor Authentication – Section 5.4.1
- Domain Name System Security Extensions (DNSSEC) Capabilities – Section 5.4.3
- Trust Zones – Section 5.4.3
- Signed Code – Section 5.4.5
- Patching and Anti-Virus – Section 5.6

3.17 Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) 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 of Protected Health Information (PHI), electronic and otherwise, for any purpose other than treatment, payment, or health care operations without the authorization of the individual or as part of an exception within HIPAA.

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

Policy ID	DHS Policy Statements	Relevant Controls
3.17.a	For those Components whose systems collect, process, or store Protected Health Information (PHI), they shall ensure that the stored information is appropriately protected in compliance with HIPAA and that access or disclosure is limited to the minimum required.	---
3.17.b	Covered Components shall work with the DHS Privacy Office, Component Privacy Office, or PPOC to ensure that privacy and disclosure policies comply with HIPAA requirements.	---

Policy ID	DHS Policy Statements	Relevant Controls
3.17.c	Covered Components shall ensure that employees with access to DHS systems that collect, process, or store PHI are trained on HIPAA requirements.	---
3.17.d	Covered Components shall establish administrative processes that can respond to complaints, requests for corrections of health information, and track disclosures of PHI.	---
3.17.e	When collecting PHI, Components shall issue a privacy notice to individuals concerning the use and disclosure of their PHI.	---

4.0 OPERATIONAL POLICIES

4.1 Personnel

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 the 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 taken to reduce the risk associated with these types of threats.

4.1.1 Citizenship, Personnel Screening, and Position Categorization

Policy ID	DHS Policy Statements	Relevant Controls
4.1.1.a	Components shall designate the position sensitivity level for all Government and contractor positions that use, develop, operate, or maintain information systems and shall determine risk levels for each contractor position. Position sensitivity levels shall be reviewed annually and revised as appropriate.	PS-2, PS-3, PS-7
4.1.1.b	Components shall ensure the incumbents of these positions have favorably adjudicated background investigations commensurate with the defined position sensitivity levels.	PS-2, PS-3, PS-7
4.1.1.c	Components shall ensure that no Federal employee is granted access to DHS systems without having a favorably adjudicated Minimum Background Investigation (MBI) as defined in DHS Instruction 121-01-007, *Personnel Suitability and Security Program.* Active duty United States Coast Guard and other personnel subject to the Uniform Code of Military Justice shall be exempted from this requirement.	PS-3
4.1.1.d	Components shall ensure that no contractor personnel shall be granted access to DHS systems without having a favorably adjudicated Background Investigation (BI) as defined in DHS Instruction 121-01-007, *Suitability Screening Requirements for Contractor Employees* and the Department of Homeland Security Acquisition Regulation (HSAR).	PS-3
4.1.1.e	Components shall ensure that only U.S. Citizens are granted access to DHS systems and networks. Exceptions to the U.S. Citizenship requirement may be granted by the Component Head or designee with the concurrence of the Office of Security and the DHS CIO, in accordance with Section 1.5.4, U.S. Citizen Exception Requests, of this policy.	PS-3

4.1.2 Rules of Behavior

Policy ID	DHS Policy Statements	Relevant Controls
4.1.2.a	Components shall ensure that rules of behavior contain acknowledgement that the user has no expectation of privacy (a “Consent to Monitor” provision) and that disciplinary actions may result from violations.	PL-4
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.	AT-1, AT-2, PL-4

4.1.3 Access to Sensitive Information

Policy ID	DHS Policy Statements	Relevant Controls
4.1.3.a	System Owners shall ensure that users of the information systems supporting their programs have a valid requirement to access these systems.	AC-2

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.

Policy ID	DHS Policy Statements	Relevant Controls
4.1.4.a	Components shall divide and separate duties and responsibilities of critical information system functions among different individuals to minimize the possibility that any one individual would have the necessary authority or system access to be able to engage in fraudulent or criminal activity.	AC-2
4.1.4.b	All individuals requiring administrator privileges shall be reviewed and approved by the appropriate AO. The AO may delegate this duty to the appropriate system owner or Program Manager.	AC-2
4.1.4.c	Individuals requiring administrator privileges shall be assigned administrator accounts separate from their normal user accounts.	AC-6
4.1.4.d	Administrator accounts shall be used only for performing required administrator duties. Individuals shall use their regular user accounts to perform all other functions not directly tied to administrator duties (checking email, accessing the Internet).	AC-6

4.1.5 Information Security Awareness, Training, and Education

Policy ID	DHS Policy Statements	Relevant Controls
4.1.5.a	Components shall establish an information security training program for users of DHS information systems.	AT-1
4.1.5.b	DHS personnel, contractors, or others working on behalf of DHS accessing DHS systems shall receive initial training and annual refresher training, in security awareness and accepted security practices. Personnel shall complete security awareness within twenty-four (24) hours of being granted a user account. If the user fails to comply, user access shall be suspended.	AT-1, AT-4
4.1.5.c	DHS personnel, contractors, or others working on behalf of DHS with significant security responsibilities (e.g., ISSOs, system administrators) shall receive initial specialized training, and annual refresher training thereafter, specific to their security responsibilities.	AT-3
4.1.5.d	Components shall maintain training records, to include name and position, type of training received, and costs of training.	AT-4
4.1.5.e	User accounts and access privileges, including access to email, shall be disabled for those DHS employees who have not received annual refresher training unless a waiver is granted by the Component CISO/ISSM.	AT-1
4.1.5.f	Components shall prepare and submit an annual security awareness training plan, as specified by the DHS Information Security Training Program Office.	AT-1
4.1.5.g	Components shall prepare and submit information security awareness reports with content, frequency, format, and distribution as specified by the DHS CISO.	AT-1
4.1.5.h	Components shall provide evidence of training by submitting copies of training schedules, training rosters, and training reports, upon request of the DHS Information Security Training Program Office.	AT-4
4.1.5.i	The DHS CISO shall review Component information security awareness programs annually.	AT-1

4.1.6 Separation From Duty

Policy ID	DHS Policy Statements	Relevant Controls
4.1.6.a	Components shall implement procedures to ensure that system accesses are revoked for DHS employees, contractors, or others working on behalf of DHS who leave the Component, are reassigned to other duties, or no longer require access.	AC-2

Policy ID	DHS Policy Statements	Relevant Controls
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.	PS-4
4.1.6.c	Accounts for personnel on extended absences shall be temporarily suspended.	AC-2
4.1.6.d	System Owners shall review information system accounts supporting their programs at least annually.	AC-2

4.2 Physical Security

4.2.1 General Physical Access

Policy ID	DHS Policy Statements	Relevant Controls
4.2.1.a	Access to DHS buildings, rooms, work areas, spaces, and structures housing information systems, equipment, and data shall be limited to authorized personnel.	PE-2
4.2.1.b	Controls for deterring, detecting, restricting, and regulating access to sensitive areas shall be in place and shall be sufficient to safeguard against possible loss, theft, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters.	PE-3
4.2.1.c	Controls shall be based on the level of classification and risk, determined in accordance with Departmental security policy as reflected in this and other relevant documents.	PE-1, PM-9
4.2.1.d	Visitors shall sign in upon entering DHS facilities that house information systems, equipment, and data, be escorted during their stay, and sign out upon leaving. Non-DHS contractor or vendor access shall be limited to those work areas requiring their presence. Visitor logs shall be maintained and available for review for one (1) year.	PE-7
4.2.1.e	These requirements shall extend to DHS assets, located at non-DHS facilities or non-DHS assets and equipment hosting DHS data.	---

4.2.2 Sensitive Facility

Policy ID	DHS Policy Statements	Relevant Controls
4.2.2.a	Facilities processing, transmitting, or storing sensitive information shall incorporate physical protection measures based on the level of risk. The risk shall be determined in accordance with Departmental security policy as reflected in this and other relevant documents.	PE-1, PM-9

4.3 Media Controls

4.3.1 Media Protection

Policy ID	DHS Policy Statements	Relevant Controls
4.3.1.a	Components shall ensure that all media containing sensitive information, including hard copy media, backup media, and removable media such as USB drives, are stored in a secure location (e.g., a locked office, room, desk, bookcase, file cabinet, locked tape device, or other storage prohibiting access by unauthorized persons) when not in use.	MP-2, MP-4, PE-1
4.3.1.b	Components shall ensure that all offsite backup media are protected as per guidance in this section.	CP-6
4.3.1.c	DHS personnel, contractors, and others working on behalf of DHS are prohibited from using any non-Government issued removable media (USB drives, in particular) or connecting them to DHS equipment or networks or to store DHS sensitive information.	MP-2
4.3.1.d	Systems requiring encryption shall comply with Section 5.5.1, Encryption, of this policy. DHS-owned USB drives shall use encryption.	IA-7, SC-13
4.3.1.e	DHS-owned removable media shall not be connected to any non-DHS information system unless the AO has determined the acceptable level of risk based on compensating controls, published acceptable use guidance and the guidance has been approved by the respective CISO/ISSM. (The respective CISO is the CISO with that system in his or her inventory.)	AC-20, MP-2, PM-9
4.3.1.f	DHS-owned USB removable media shall not be connected to any non-DHS information system.	AC-20, MP-2
4.3.1.g	Components shall follow established procedures to ensure that paper and electronic outputs from systems containing sensitive information are protected.	MP-1
4.3.1.h	Users shall ensure proper protection of printed output. Printing of sensitive documents shall occur only when a trusted person is attending the printer.	SI-12

Policy ID	DHS Policy Statements	Relevant Controls
4.3.1.i	Components shall follow the procedures established by DHS MD 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, for the transportation or mailing of sensitive media.	MP-5

4.3.2 Media Marking and Transport

Policy ID	DHS Policy Statements	Relevant Controls
4.3.2.a	Media determined by the information owner to contain sensitive information shall be appropriately marked in accordance with DHS MD 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*.	MP-3
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.	MP-5

4.3.3 Media Sanitization and Disposal

Policy ID	DHS Policy Statements	Relevant Controls
4.3.3.a	Components shall ensure that any information systems storage medium containing sensitive information is sanitized using approved sanitization methods before it is disposed of, reused, recycled, or returned to the owner or manufacturer.	MP-6
4.3.3.b	Components shall maintain records of the sanitization and disposition of information systems storage media.	MP-6
4.3.3.c	Components shall periodically test degaussing equipment to verify that the equipment is functioning properly.	MP-6

4.3.4 Production, Input/Output Controls

Policy ID	DHS Policy Statements	Relevant Controls
4.3.4.a	Components shall follow established procedures to ensure that sensitive information cannot be accessed or stolen by unauthorized individuals.	SI-12
4.3.4.b	These procedures shall address not only the paper and electronic outputs from systems but also the transportation or mailing of sensitive media.	SI-12

4.4 Voice Communications Security

4.4.1 Private Branch Exchange

Policy ID	DHS Policy Statements	Relevant Controls
4.4.1.a	Components shall provide adequate physical and information security for all DHS-owned Private Branch Exchanges (PBX). (Refer to NIST SP 800-24, *PBX Vulnerability Analysis*, for guidance on detecting and fixing vulnerabilities in PBX systems.)	CM-2

4.4.2 Telephone Communications

Policy ID	DHS Policy Statements	Relevant Controls
4.4.2.a	Components shall develop guidance for discussing sensitive information over the telephone. Guidance shall be approved by a senior Component official and is subject to review and approval by the DHS CISO. Under no circumstances shall classified national security information be discussed over unsecured telephones.	PL-4

4.4.3 Voice Mail

Policy ID	DHS Policy Statements	Relevant Controls
4.4.3.a	Sensitive information shall not be communicated over nor stored in voice mail.	PL-4

4.5 Data Communications

4.5.1 Telecommunications Protection Techniques

Policy ID	DHS Policy Statements	Relevant Controls
4.5.1.a	Components shall carefully select the telecommunications protection techniques that meet their information security needs, in the most cost-effective manner, consistent with Departmental and Component information system security policies. Approved protected network services (PNS) may be used as cost-effective alternatives to the use of encryption for sensitive information requiring telecommunications protection.	CM-2

4.5.2 Facsimiles

Policy ID	DHS Policy Statements	Relevant Controls
4.5.2.a	Components shall implement and enforce technical controls for fax technology and systems (including fax machines, servers, gateways, software, and protocols) that transmit and receive sensitive information.	SC-1, SC-7, SC-8, SC-9
4.5.2.b	Components shall configure fax servers to ensure that incoming lines cannot be used to access the network or any data on the fax server.	AC-4

4.5.3 Video Teleconferencing

Policy ID	DHS Policy Statements	Relevant Controls
4.5.3.a	Components shall implement controls to ensure that only authorized individuals are able to participate in each videoconference.	AC-3, PE-3
4.5.3.b	Components shall ensure that appropriate transmission protections, commensurate with the highest sensitivity of information to be discussed, are in place throughout any video teleconference.	SC-8, SC-9
4.5.3.c	Video teleconferencing equipment and software shall be disabled when not in use.	AC-3, PE-3

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).

Policy ID	DHS Policy Statements	Relevant Controls
4.5.4.a	Prior to implementing voice over data network technology, Components shall conduct rigorous risk assessments and security testing and provide a business justification for their use. Any systems that employ this technology shall be accredited for this purpose with residual risks clearly identified.	SC-19, PM-9
4.5.4.b	Voice over data network implementations shall have sufficient redundancy to ensure network outages do not result in the loss of both voice and data communications.	SC-19
4.5.4.c	Components shall ensure appropriate identification and authentication controls, audit logging, and integrity controls are implemented on every element of their voice over data networks.	SC-19

Policy ID	DHS Policy Statements	Relevant Controls
4.5.4.d	Components shall ensure that physical access to voice over data network elements is restricted to authorized personnel.	SC-19

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 portable electronic devices (PED) capable of storing, processing, or transmitting sensitive information (e.g., personal digital assistants [PDA], 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)

Policy ID	DHS Policy Statements	Relevant Controls
4.6.a	Wireless network communications technologies are prohibited from use within DHS unless the appropriate AO specifically approves a technology and application.	AC-18
4.6.b	Components using Public Key Infrastructure (PKI)-based encryption on wireless systems, wireless PEDs, and wireless tactical systems shall implement and maintain a key management plan approved by the DHS PKI Policy Authority.	IA-5, SC-12

4.6.1 Wireless Systems

Wireless system policy and procedures are described more completely in Attachment Q1 (*Wireless Systems*) to the DHS 4300A *Sensitive Systems Handbook*.

Policy ID	DHS Policy Statements	Relevant Controls
4.6.1.a	Annual information security assessments shall be conducted on all approved wireless systems. Wireless information security assessments shall enumerate vulnerabilities, risk statements, risk levels, and corrective actions.	CA-2, PM-9
4.6.1.b	A POA&M shall be developed to address wireless information security vulnerabilities. These plans shall prioritize corrective actions and implementation milestones in accordance with defined risk levels.	CA-5, PM-4, PM-9
4.6.1.c	Components shall identify countermeasures to denial-of-service attacks and complete a risk based evaluation prior to approving the use of a wireless PED	AC-19, PM-9, SC-5
4.6.1.d	SPs shall adopt a defense-in-depth strategy that integrates firewalls, screening routers, wireless intrusion detection systems, antivirus software, encryption, strong authentication, and cryptographic key management to ensure information security solutions and secure connections to external interfaces are consistently enforced.	SI-3
4.6.1.e	Legacy wireless systems that are not compliant with DHS information security policy shall implement a migration plan to outline the provisions, procedures, and restrictions for transitioning these systems to DHS-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception to policy from the DHS CISO.	CA-5
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 annually.	AC-18, PM-5
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.	AC-18

4.6.2 Wireless Portable Electronic Devices

Wireless PEDs include PDAs, smart telephones, two-way pagers, handheld radios, cellular telephones, PCS devices, multifunctional wireless devices, portable audio/video recording devices with wireless capability, scanning devices, messaging devices, and any other wireless clients capable of storing, processing, or transmitting sensitive information.

Wireless PED policy and procedures are described more completely in Attachment Q2 (*Wireless Portable Electronic Devices*) to the DHS 4300A *Sensitive Systems Handbook*.

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.a	The use of wireless PEDs and accessory devices in areas where sensitive or classified information is discussed, maintained, or distributed is prohibited unless specifically authorized by the AO in writing.	AC-19, PL-4
4.6.2.b	Wireless PEDs shall not be tethered or otherwise physically or wirelessly connected to the DHS-wired core network without written consent from the AO.	AC-18, AC-19
4.6.2.c	Wireless PEDs shall not be used to store, process, or transmit combinations, personal identification numbers (PIN), or sensitive information in unencrypted formats.	AC-19, IA-5, IA-7
4.6.2.d	Wireless PEDs such as BlackBerry devices and smart phones shall implement strong authentication, data encryption, and transmission encryption technologies. Portable electronic devices such as BlackBerry devices and smart phones shall be password-protected, with a security timeout period established. For BlackBerry devices, the security timeout shall be set to ten (10) minutes.	AC-19, IA-7, SC-8, SC-9, SC-13
4.6.2.e	SPs shall promulgate the provisions, procedures, and restrictions for using wireless PEDs to download mobile code in an approved manner.	SC-18
4.6.2.f	Wireless PEDs shall be operated only when current DHS TRM-approved versions of antivirus software and software patches are installed.	SI-3
4.6.2.g	Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless PED being approved for use.	SC-5 SC-7
4.6.2.h	Components shall maintain a current inventory of all approved wireless PEDs in operation.	PM-5
4.6.2.i	Wireless PEDs shall be cleared of all information before being reused by another individual, office, or Component within DHS or before they are surplused; wireless PEDs that are being disposed of, recycled, or returned to the owner or manufacturer shall first be sanitized using approved procedures.	MP-6
4.6.2.j	Legacy wireless PEDs that are not compliant with DHS information security policy shall implement a migration plan that outlines the provisions, procedures, and restrictions for transitioning these wireless PEDs to DHS-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception from the DHS CISO.	CA-5 CA-6
4.6.2.k	Components shall ensure that personally owned PEDs and Government-owned PEDs not authorized to process classified information are not permitted in conference rooms or secure facilities where classified information is discussed.	AC-19, PE-18

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.l	The AO shall approve the use of Government-owned PEDs to process, store, or transmit sensitive information.	CA-6
4.6.2.m	The use of add-on devices, such as cameras and recorders, is not authorized unless approved by the AO. Functions that can record or transmit sensitive information via video, Infrared (IR), or Radio Frequency (RF) shall be disabled in areas where sensitive information is discussed.	AC-19, CM-7, PE-18, SC-7

4.6.2.1 Cellular Phones

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.1.a	Components shall develop guidance for discussing sensitive information on cellular phones. Guidance shall be approved by a senior Component official and is subject to review by the DHS CISO. Under no circumstances shall classified information be discussed on cellular phones.	PL-4

4.6.2.2 Pagers

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.2.a	Pagers shall not be used to transmit sensitive information.	PL-4

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.

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.3.a	Functions that cannot be encrypted using approved cryptographic modules shall not be used to process, store, or transmit sensitive information.	AC-19, SC-8, SC-9, SC-12
4.6.2.3.b	Functions that transmit or receive video, IR, or radio frequency RF)signals shall be disabled in areas where sensitive information is discussed.	AC-19, PE-18
4.6.2.3.c	Short Message Service (SMS) and Multimedia Messaging Service (MMS) shall not be used to process, store, or transmit sensitive information, and shall be disabled whenever possible.	---

4.6.3 Wireless Tactical Systems

Wireless tactical systems include 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 the DHS 4300A *Sensitive Systems Handbook*.

Policy ID	DHS Policy Statements	Relevant Controls
4.6.3.a	AOs shall be immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents.	CM-3
4.6.3.b	Wireless tactical systems shall implement strong identification, authentication, and encryption.	IA-2, IA-7, SC-8, SC-9
4.6.3.c	Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless tactical system being approved for use.	SC-5
4.6.3.d	Components shall maintain a current inventory of all approved wireless tactical systems in operation.	PM-5
4.6.3.e	Legacy tactical wireless systems that are not compliant with DHS information security policy shall implement a migration plan to outline the provisions, procedures, and restrictions for transitioning these systems to DHS-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception from the DHS CISO, as appropriate.	---
4.6.3.f	The security configuration of LMR subscriber units shall be validated via over-the-air-rekeying (OTAR) or hard rekey using a crypto-period no longer than 180 days.	SC-12
4.6.3.g	All LMR systems shall comply with Project 25 (P25, EIA/TIA-102) security standards where applicable.	CM-2

4.6.4 Radio Frequency Identification

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 Attachment Q4 (S*ensitive RFID Systems*) to the DHS 4300A *Sensitive Systems Handbook.*

Policy ID	DHS Policy Statements	Relevant Controls
4.6.4.a	Components implementing RFID systems shall assess hazards of electromagnetic radiation to fuel, ordinance, and personnel before deployment of the RFID technology.	PE-18
4.6.4.b	Components shall limit data stored on RFID tags to the greatest extent possible, recording information beyond an identifier only when required for the application mission. When data beyond an identifier is stored on a tag, the tag's memory shall be protected by access control.	AC-6, PL-5
4.6.4.c	Components shall develop a contingency plan, such as the use of a fallback identification technology, to implement in case of an RFID security breach or system failure.	---
4.6.4.d	Components shall identify and implement appropriate operational and technical controls to limit unauthorized tracking or targeting of RFID-tagged items when these items are expected to travel outside the Component's physical perimeter.	AC-14
4.6.4.e	When the RFID system is connected to a DHS data network, Components shall implement network security controls to segregate RFID network elements such as RFID readers, middleware, and databases from other non-RFID network hosts.	CM-6
4.6.4.f	Components implementing RFID technology shall determine whether or not tag cloning is a significant business risk. If such a significant risk exists, then tag transactions shall be cryptographically authenticated.	IA-7, PM-9, RA-3

4.7 Overseas Communications

Policy ID	DHS Policy Statements	Relevant Controls
4.7.a	Where required or appropriate, all communications outside of the United States and its territories shall be in accordance with the Department of State Foreign Affairs Manual (FAM), 12 FAM 600, *Information Security Technology*.	---

4.8 Equipment

4.8.1 Workstations

Policy ID	DHS Policy Statements	Relevant Controls
4.8.1.a	Components shall configure *workstations* to either log off, or activate a password-protected lock, or password-protected screensaver within fifteen (15) minutes of user inactivity.	AC-11, CM-6
4.8.1.b	Components shall ensure that workstations are protected from theft.	PE-3
4.8.1.c	Users shall either log off or lock their workstations when unattended.	---

4.8.2 Laptop Computers and Other Mobile Computing Devices

Policy ID	DHS Policy Statements	Relevant Controls
4.8.2.a	Information stored on any laptop computer or other mobile computing device that may be used in a residence or on travel shall use encryption in accordance with Section 5.5.1, Encryption, for data at rest and in motion. Passwords, tokens and Smart Cards shall not be stored on or with the laptop or other mobile computing device.	AC-19, IA-2, SC-12
4.8.2.b	Laptop computers shall be powered down when not in use (due to volatile memory vulnerabilities).	AC-19, PL-4
4.8.2.c	Laptop computers and other mobile computing devices in offices shall be secured when unattended via a locking cable, locked office, or locked cabinet or desk.	AC-19, PE-3, PL-4
4.8.2.d	Users shall obtain the written approval of the office director before taking a laptop computer or other mobile computing device outside of the United States or its territories.	AC-19, PL-4

4.8.3 Personally Owned Equipment and Software

Policy ID	DHS Policy Statements	Relevant Controls
4.8.3.a	Personally owned equipment and software shall not be used to process, access, or store sensitive information without the written prior approval of the AO.	SA-6
4.8.3.b	Equipment that is not owned or leased by the Federal Government, or operated by a contractor on behalf of the Federal Government, shall not be connected to DHS equipment or networks without the written prior approval of the Component CISO/ISSM.	SA-9

Policy ID	DHS Policy Statements	Relevant Controls
4.8.3.c	Any device that has been obtained through civil or criminal asset forfeiture shall not be used as part of a DHS information system nor used to process DHS data.	AC-20

4.8.4 Hardware and Software

Policy ID	DHS Policy Statements	Relevant Controls
4.8.4.a	Components shall ensure that DHS information systems follow the hardening guides for operating systems and the configuration guides for applications promulgated by the DHS CISO. DHS Sensitive Systems Handbook, Enclosure 1, includes the DHS Secure Baseline Configuration Guides.	CM-2, CM-6
4.8.4.b	Components shall limit access to system software and hardware to authorized personnel.	AC-3, CM-5
4.8.4.c	Components shall test, authorize, and approve all new and revised software and hardware prior to implementation in accordance with their Configuration Management Plan.	CM-2, CM-3
4.8.4.d	Components shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches, and eliminating or disabling unnecessary services.	CM-3, RA-5
4.8.4.e	Components shall ensure that maintenance ports are disabled during normal system operation and enabled only during approved maintenance activities.	MA-1
4.8.4.f	System libraries shall be managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.	SI-7
4.8.4.g	Components shall develop maintenance policy and procedures.	MA-1
4.8.4.h	If cleared maintenance personnel are not available, a trusted DHS employee with sufficient technical knowledge to detect and prevent unauthorized modification to the information system or its network shall monitor and escort the maintenance personnel during maintenance activities. This situation shall only occur in exceptional cases. Components shall take all possible steps to ensure that trusted maintenance personnel are available.	MA-5
4.8.4.i	Maintenance using a different user's identity may be performed only when the user is present. The *user* shall log in and observe the maintenance actions at all times. *Users shall not share their authentication information with maintenance personnel.*	MA-5

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

Policy ID	DHS Policy Statements	Relevant Controls
4.8.5.a	DHS employees may use Government office equipment and DHS systems/computers for authorized purposes only. "Authorized use" includes limited personal use as described in DHS MD 4600.1, *Personal Use of Government Office Equipment*, and DHS MD 4900, *Individual Use and Operation of DHS Information Systems/Computers*.	---
4.8.5.b	Limited personal use of DHS email and Internet services is authorized for DHS employees as long as this use does not interfere with official duties, inhibit the security of information and information systems, or cause degradation of network services. Specifically prohibited activities include streaming of audio or video, social networking, peer-to-peer networking, software or music sharing/piracy, online gaming, webmail, Instant Messaging (IM), hacking, and the viewing of pornography or other offensive content. DHS users shall comply with the provisions of DHS MD 4500.1, *DHS E-mail Usage*, and DHS MD 4400.1, *DHS Web and Information Systems*.	---
4.8.5.c	Anyone granted user account access to any DHS information system (including DHS employees, contractors, and others working on behalf of DHS) shall have no expectations of privacy associated with its use. By completing the authentication process, the user acknowledges his or her consent to monitoring.	AC-8
4.8.5.d	The use of Government office equipment and DHS systems/computers constitutes consent to monitoring and auditing of the equipment/systems at all times. Monitoring includes the tracking of internal 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.	AC-8
4.8.5.e	DHS users are required to sign rules of behavior prior to being granted system accounts or access to DHS systems or data. The rules of behavior shall contain a "Consent to Monitor" provision and an acknowledgement that the user has no expectation of privacy.	PL-4
4.8.5.f	Contractors, others working on behalf of DHS, or other non-DHS employees are not authorized to use Government office equipment or information systems/computers for personal use, unless limited personal use is specifically permitted by the contract or memorandum of agreement. When so authorized, the limited personal use policies of this section and the provisions of DHS MD 4600.1, DHS MD 4900, DHS MD 4400.1, and DHS MD 4500.1 shall apply.	---

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.

Policy ID	DHS Policy Statements	Relevant Controls
4.8.6.a	Components shall ensure that wireless capabilities for peripheral equipment are disabled. This applies all to peripherals connected to any DHS network or to systems processing or hosting DHS sensitive data.	CM-7
4.8.6.b	In cases where valid mission requirements or equipment limitations prevent disabling wireless capabilities, Components shall comply with all requirements outlined in Section 4.6, Wireless Communication *and* obtain a waiver or exception in accordance with this policy.	CM-7

4.9 Department Information Security Operations

The DHS EOC is the central coordinating and reporting authority for all Sensitive and National Security computer security incidents throughout the Department. The HSDN SOC shall report incidents to the DHS EOC through appropriate channels to protect data classification. The HSDN SOC is subordinate to the DHS EOC, acting as the central coordinating and reporting authority for all SECRET computer security incidents throughout the Department.

Policy ID	DHS Policy Statements	Relevant Controls
4.9.a	It is the policy of DHS that employees, contractors, or others working on behalf of DHS have no privacy expectations associated with the use of any DHS network, system, or application. This policy is further extended to anyone who is granted account access to any network, system, or application in use in the Department. By completing the account log in process the account owner acknowledges their consent to monitoring.	AC-8, PL-4
4.9.b	Component SOCs and the HSDN SOC shall be operationally subordinate to the DHS EOC. The DHS EOC shall provide operational oversight and guidance.	IR-1
4.9.c	The DHS EOC or Component SOCs shall lead the coordination and administration of Department and Component policy enforcement points, such as firewalls.	SC-7
4.9.d	The DHS EOC shall implement the Department logging strategy, coordinated with Component SOCs, to enable endpoint visibility and Departmental situational awareness.	---
4.9.e	All SOCs shall have the capability to process intelligence information at the collateral level or above. The DHS EOC and Component SOCs shall have the ability to process SECRET level information continuously and shall have the capability to receive TS/SCI information.	IR-4
4.9.f	SOCs shall ensure that personnel are appropriately cleared to access Joint Worldwide Intelligence Communications System (JWICS). SOC managers are free to determine the number and type of personnel to be cleared, but at least	IR-4

Policy ID	DHS Policy Statements	Relevant Controls
	one cleared person shall be available per shift. (This person may be on call.) A Government officer shall be available continuously for incident response and management.	
4.9.g	All Department SOCs shall establish and maintain a forensic capability as outlined in the DHS Enterprise Operations Concept of Operations (EOC CONOPS).	IR-7
4.9.h	Department information security operations shall provide a vulnerability management capability. DHS EOC provides Information Security Vulnerability Management (ISVM) messages and vulnerability assessment capabilities. Component SOCs shall develop a robust vulnerability management capability to compliment the DHS EOC.	SI-5
4.9.i	Component CISOs shall ensure that the DHS CISO is kept apprised of all pertinent matters involving the security of information systems and that security-related decisions and information are distributed to the ISSOs and other appropriate persons.	SI-5
4.9.j	Component SOCs shall report operationally to the respective Component CISO. Each CISO shall exercise oversight over their Components' information security operations functions, including the Component SOCs.	IR-1
4.9.k	The DHS EOC shall report operationally to the DHS CISO.	

4.10 Security Incidents and Incident Response and Reporting

Policy ID	DHS Policy Statements	Relevant Controls
4.10.a	Components shall establish and maintain a continuous incident response capability.	IR-1
4.10.b	Components shall report *significant incidents* to the DHS EOC by calling (703) 921-6505 as soon as possible but not later than one (1) hour from "validation" (e.g., a security event being confirmed as a security incident). Other means, such as the EOC ONLINE portal (https://eoconline.dhs.gov) are acceptable, but the Component shall positively verify that the notification is received and acknowledged by the DHS EOC.	IR-6
4.10.c	Significant HSDN incidents shall be documented with a preliminary report that shall be provided to the HSDN Government Watch Officer or DHS EOC within one hour. An initial detailed report shall be provided to the DHS EOC as soon as possible but not later than one hour from "validation" via secure communications. Subsequent updates and status reports shall be provided to the DHS EOC every twenty-four (24) hours via HSDN SOC ONLINE until incident resolution or when new information is discovered. Significant	IR-6

Policy ID	DHS Policy Statements	Relevant Controls
	incidents are reported individually on a per incident basis and shall not be reported in the monthly summary report. Additional guidance is located in DHS 4300A Attachment F, *Incident Response and Reporting,* Section 3.0.	
4.10.d	Components shall report minor incidents on systems in the weekly incident report. SBU systems may report via the DHS EOC portal (https://eoconline.dhs.gov). Components with no portal access shall report minor incidents via email to dhs.soc@dhs.gov. HSDN incidents or incidents involving SECRET information shall be documented in a summary report via the HSDN DHS EOC portal.	IR-6
4.10.e	DHS personnel shall follow DHS CISO procedures for detecting, reporting, and responding to information security incidents in accordance with the DHS EOC CONOPS. Reports shall be classified at the highest classification level of the information contained in the document. Unsanitized reports shall be marked and handled appropriately.	IR-1
4.10.f	If a DHS Component has no incidents to report for a given week, a weekly “No Incidents” report shall be sent to the EOC.	IR-6
4.10.g	The DHS EOC shall report incidents to US-CERT, in accordance with the DHS EOC CONOPS. Components shall not send incident reports directly to US-CERT.	IR-6
4.10.h	The DHS EOC shall receive classified spillage incident reports, and support the DHS CSO for containment and cleanup. All classified spillages are significant incidents.	IR-6
4.10.i	The DHS EOC shall maintain information security “playbooks,” that is, checklists that implement procedures and provide guidance on how to respond rapidly to developing incidents.	IR-1
4.10.j	The DHS EOC shall respond to detected faults, attacks, events, or incidents and communicate incident reports to external organizations that may be affected.	IR-1
4.10.k	Components shall maintain a full SOC and CSIRC capability or outsource this capability to the DHS EOC. The DHS EOC 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.*	IR-7
4.10.l	Components shall develop and publish internal computer security incident response plans and incident handling procedures, and provide copies to the DHS CSIRC. These procedures shall include a detailed CM process for modification of security device configurations.	IR-1

Policy ID	DHS Policy Statements	Relevant Controls
4.10.m	Component Heads shall take corrective actions when security incidents and violations occur and shall hold personnel accountable for intentional transgressions.	IR-1
4.10.n	The DHS EOC shall monitor and report incident investigation and incident remediation activities to the DHS CIO and CISO in accordance with the DHS EOC CONOPS until the incident is closed.	IR-5
4.10.o	The DHS CISO shall determine the frequency and content of security incident reports.	IR-6
4.10.p	The Component CSIRC shall report incidents only to the DHS EOC and to no other external agency or organization.	IR-6
4.10.q	The DHS CISO shall publish Incident Response Testing and Exercise scenarios as required.	IR-1
4.10.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.	IR-3

4.10.1 Law Enforcement Incident Response

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

Policy ID	DHS Policy Statements	Relevant Controls
4.10.1.a	Components shall coordinate all external law enforcement involvements through the DHS EOC and obtain guidance from the DHS EOC before contacting local law enforcement. Exceptions are only made during emergencies where there is risk to life, limb, or destruction of property. In cases of emergency notification, the Component shall notify the DHS EOC as soon as possible, by the most expedient means available.	IR-6
4.10.1.b	Security Incidents may include law enforcement (LE) or counter intelligence (CI) elements, such as maintaining a chain of custody. All incidents containing a LE/CI aspect shall be coordinated with the DHS CSO through the DHS EOC.	IR-6

4.11 Documentation

Policy ID	DHS Policy Statements	Relevant Controls
4.11.a	Components shall ensure that information systems and networks are appropriately documented in such a way as to allow others to understand system operation and configuration.	CM-8
4.11.b	System Owners shall update system documentation annually or whenever system changes occur. Such changes include: • A vulnerability scan of the information system; • New threat information; • Weaknesses or deficiencies discovered in currently deployed security controls after an information system breach; • A redefinition of mission priorities or business objectives resulting in a change to the security category of the information system; and A change in the information system (e.g., adding new hardware, software, or firmware; establishing new connections) or the system's environment of operation	CM-3, CM-8, SA-5
4.11.c	Documentation shall be kept on hand and be accessible to authorized personnel (including auditors) at all times.	CM-3
4.11.d	System documentation may be categorized as Sensitive if deemed appropriate by the Component CISO/ISSM. This category shall not be used as a means to restrict access to auditors or other authorized personnel.	CM-3

4.12 Information and Data Backup

Policy ID	DHS Policy Statements	Relevant Controls
4.12.a	The policies in this document, including Security Authorization Process requirements, apply to any devices that process or host DHS data.	---
4.12.b	Component CISOs/ISSMs shall determine whether or not automated process devices shall be included as part of an information system's Security Authorization Process requirements.	---
4.12.c	. This policy directive and the DHS 4300A Sensitive Systems Handbook apply 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. This includes prototypes, telecommunications systems, and all systems in all phases of the System Engineering Life Cycle.	---

4.13 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.

Policy ID	DHS Policy Statements	Relevant Controls
4.13.a	The policies in this document apply to any networked devices that contain information technology, including copiers, facsimile machines, and alarm control systems.	---
4.13.b	Components shall ensure that network printers and facsimile machines are updated to the latest version of their firmware/software at least annually.	CM-2
4.13.c	Components shall ensure that network printers, copiers, and facsimile machines shall be configured for least required functionality.	CM-7
4.13.d	Components shall ensure that each network printer, copier, and facsimile machine is within the system definition of a DHS information system that has a current ATO.	CM-8
4.13.e	Components shall ensure that remote maintenance of network printers, copiers, and facsimile machines is conducted only from within DHS networks. If maintenance planning does not include performing remote maintenance, Components shall ensure that remote maintenance capabilities are disabled.	MA-4
4.13.f	Components shall ensure that network printers, copiers, and facsimile machines are configured to restrict administrator access to authorized individuals or groups.	MA-5
4.13.g	Components shall ensure that maintenance or disposal of network printers, copiers, or facsimile machines, approved for sensitive reproduction, is performed only while escorted by a properly cleared person with knowledge to detect any inappropriate action.	MA-5
4.13.h	Components shall ensure that memory and hard drives do not leave the facility; they are to be replaced and the old part destroyed as sensitive media.	MP-6
4.13.i	Components shall locate network printers, copiers, and facsimile machines approved to process sensitive information in areas where access can be controlled when paper output is being created.	PE-18
4.13.j	Any multifunction device connected to a DHS network or other information system containing sensitive data shall have the inbound dial in capabilities disabled.	AC-17

5.0 TECHNICAL POLICIES

The design of information systems that process, store, or transmit sensitive information shall include the automated security features discussed in this section. Security safeguards shall be in place to ensure that each person having access to sensitive information systems is individually accountable for his or her actions while utilizing the system.

5.1 Identification and Authentication

Policy ID	DHS Policy Statements	Relevant Controls
5.1.a	Components shall ensure that user access is controlled and limited based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.	IA-1, IA-2
5.1.b	For information systems requiring authentication controls, Components shall ensure that the information system is configured to require that each user be authenticated before information system access occurs.	IA-1, IA-2
5.1.c	For systems with low impact for the confidentiality security objective, Components shall disable user identifiers after ninety (90) days of inactivity; for systems with moderate and high impacts for the confidentiality security objective, Components shall disable user identifiers after forty-five (45) days of inactivity.	IA-4
5.1.d	DHS users shall not share identification or authentication materials of any kind, nor shall any DHS user allow any other person to operate any DHS system by employing the user’s identity.	IA-5
5.1.e	All user authentication materials shall be treated as sensitive material and shall carry a classification as high as the most sensitive data to which that user is granted access using that authenticator.	IA-7
5.1.f	Components shall implement strong authentication on servers, for system administrators and personnel with significant security responsibilities, within six (6) months of the Component’s implementation of Homeland Security Presidential Directive (HSPD) HSPD-12.	IA-2

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), shall be cost-justified through the risk assessment process.

Policy ID	DHS Policy Statements	Relevant Controls
5.1.1.a	In those systems where user identity is authenticated by password, the system ISSO shall determine and enforce appropriate measures to ensure that strong passwords are used.	IA-5
5.1.1.b	The ISSO shall determine and enforce the appropriate frequency for changing passwords in accordance with appropriate guidance documentation (if published). In the absence of specific guidance documentation, passwords shall not remain in effect longer than ninety (90) days.	IA-5
5.1.1.c	DHS users shall not share personal passwords.	IA-5
5.1.1.d	Use of group passwords is limited to situations dictated by operational necessity or critical for mission accomplishment. Use of a group User ID and password shall be approved by the appropriate AO.	IA-4
5.1.1.e	Components shall prohibit passwords from being embedded in scripts or source code.	IA-5
5.1.1.f	Components shall ensure that all passwords are stored in encrypted form.	IA-5

The use of a personal password by more than one individual is prohibited throughout the DHS. However, it is recognized 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.

5.2 Access Control

Policy ID	DHS Policy Statements	Relevant Controls
5.2.a	Components shall implement access control policy and procedures that provide protection from unauthorized alteration, loss, unavailability, or disclosure of information.	AC-1
5.2.b	Access control shall follow the principles of least privilege and separation of duties and shall require users to use unique identifiers. *Social Security Numbers shall not be used as login IDs.*	AC-2, IA-1
5.2.c	Users shall not provide their passwords to anyone, including system administrators.	IA-5
5.2.d	Emergency and temporary access authorization shall be strictly controlled and shall be approved by the Component CISO/ISSM or his/her designee prior to being granted.	AC-2

Policy ID	DHS Policy Statements	Relevant Controls
5.2.e	System Owners shall ensure that users are assigned unique account identifiers.	AC-2, IA-4
5.2.f	DHS systems with a FIPS 199 confidentiality categorization of high shall limit the number of concurrent sessions for any user to one (1).	AC-10

5.2.1 Automatic Account Lockout

Components shall configure each information system to lock a user's account for a specified period following a specified number of consecutive failed logon attempts. Users shall be locked from their account for a period of twenty (20) minutes after three consecutive failed logon attempts during a twenty-four (24) hour time period. All failed logon attempts must be recorded in an audit log and periodically reviewed.

Policy ID	DHS Policy Statements	Relevant Controls
5.2.1.a	Components shall configure accounts to automatically lock a user's *account* after three consecutive failed logon attempts during a twenty-four (24) hour time period.	AC-7
5.2.1.b	The automatic lockout period for accounts locked due to failed login attempts shall be set for twenty (20) minutes.	AC-7
5.2.1.c	Components shall establish a process for manually unlocking accounts prior to the expiration of the twenty (20) minute period, after sufficient user identification is established. This may be accomplished through the help desk.	AC-7

5.2.2 Automatic Session Termination

A session refers to a connection between a terminal device (workstation, laptop, PED) and a networked application or system. (This does not include a direct connection to a DHS network, such as authenticating from a device that is directly connected to a DHS network.) A session also refers to accessing an application or system through the DHS network, such as a database or networked application. When a session is locked, the user may resume activity by reauthenticating. When a session is terminated, the user is disconnected and all unsaved work is lost.

Policy ID	DHS Policy Statements	Relevant Controls
5.2.2.a	Components shall configure networked applications or systems to automatically lock any user session in accordance with the appropriate configuration guide. In the absence of configuration guidance, the session shall lock following twenty (20) minutes of inactivity.	AC-11

Policy ID	DHS Policy Statements	Relevant Controls
5.2.2.b	Locked sessions shall remain locked until the user re-authenticates.	AC-11
5.2.2.c	Sessions shall automatically be terminated after sixty (60) minutes of inactivity.	SC-10

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.

Policy ID	DHS Policy Statements	Relevant Controls
5.2.3.a	Systems internal to the DHS network shall display a warning banner stipulated by the DHS CISO.	AC-8
5.2.3.b	Systems accessible to the public shall provide both a security and privacy statement at every entry point.	AC-8

5.3 Auditing

Policy ID	DHS Policy Statements	Relevant Controls
5.3.a	Audit records shall be sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. Audit records shall be reviewed as specified in the SP. The audit record shall contain at least the following information: - Identity of each user and device accessing or attempting to access the system - Time and date of the access and the logoff - Activities that might modify, bypass, or negate information security safeguards - Security-relevant actions associated with processing - All activities performed using an administrator's identity	AU-3
5.3.b	Audit records for financial systems or for systems hosting or processing PII shall be reviewed each month. Unusual activity or unexplained access attempts shall be reported to the System Owner and Component CISO/ISSM.	AU-6
5.3.c	Components shall ensure that their audit records and audit logs are protected from unauthorized modification, access, or destruction.	AU-9
5.3.d	Components shall ensure that audit logs are recorded and retained in accordance with the Component's Record Schedule or the DHS Records Schedule. At a minimum audit trail records shall be maintained *online* for at least ninety (90) days. *Audit trail records shall be preserved for a period of seven (7) years* as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease.	AU-11
5.3.e	Components shall evaluate the system risks associated with extracts of PII from databases. If the risk is determined to be sufficiently high, a procedure shall be developed for logging computer-readable data extracts. If logging these extracts is not possible, this determination shall be documented, and compensating controls identified in the SP.	AU-1, AU-2, AU-3, PM-9
5.3.f	Component SOCs shall implement both general and threat-specific logging.	AU-1

5.4 Network and Communications Security

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 away from their normal work locations. However, there are significant security risks associated with remote access and dial-in capabilities. Proper procedures can help mitigate these risks.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.1.a	Data communication connections via modems shall be limited and shall be tightly controlled as such connections can be used to circumvent security controls intended to protect DHS networks. Data communication connections are not allowed unless they have been authorized by the Component CISO/ISSM. Approved remote access to DHS networks shall only be accomplished through equipment specifically approved for that purpose. Tethering through wireless PEDs is prohibited unless approved by the appropriate AO.	AC-4, AC-17, AU-2 SC-7, SC-8, SC-9
5.4.1.b	Components shall centrally manage all remote access and dial-in connections to their systems and shall ensure that remote access and approved dial-in capabilities provide strong authentication, two-factor authentication, audit capabilities, and protection for sensitive information throughout transmission. DHS has an immediate goal that remote access shall only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. Any two-factor authentication shall be based on Department-controlled certificates or hardware tokens issued directly to each authorized user. Remote access solutions shall comply with the encryption requirements of FIPS 140-2, *Security Requirements for Cryptographic Modules*. See Privacy Controls Section (Section 3.14) for additional requirements involving remote access of PII.	AC-4, AC-17, AU-2 SC-7, SC-8, SC-9
5.4.1.c	Remote access of PII shall comply with all DHS requirements for sensitive systems, including strong authentication. Strong authentication shall be accomplished via virtual private network (VPN) or equivalent encryption and two-factor authentication. The Risk Assessment and SP shall document any remote access of PII, and the remote access shall be approved by the AO prior to implementation.	AC-4, AC-17, AU-2 SC-7, SC-8, SC-9
5.4.1.d	Remote access of PII shall not permit the download and remote storage of information unless the requirements for the use of removable media with sensitive information have been addressed. All downloads shall follow the concept of least privilege and shall be documented with the SP.	---

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. 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.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.2.a	Components shall provide continuous monitoring of their networks for security events or outsource this requirement to the DHS EOC. Monitoring includes interception and disclosure as required for the rendition of service or to protect the Department’s or Component’s rights or property. Service observing or random monitoring shall not be used except for mechanical or service quality control checks. (As per the Electronic Communications Privacy Act) In this instance, “rights” refers to ownership or entitlements or property or information as in intellectual property.	SI-4
5.4.2.b	The DHS EOC shall administer and monitor DHS intrusion detection system (IDS) sensors and security devices.	SI-4
5.4.2.c	Component SOCs shall administer and monitor Component IDS sensors and security devices.	SI-4

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. This applies to systems that pass 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. It does not include instances of a user logging on to add or retrieve data, nor users accessing web-enabled applications through a browser.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.3.a	Components shall ensure that appropriate identification and authentication controls, audit logging, and access controls are implemented on every network element.	AC-1, AC-2, AU-1, AU-2, IA-1, IA-2
5.4.3.b	Interconnections between DHS and non-DHS systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or interconnection security agreements.	CA-3
5.4.3.c	Components shall document all interconnections to the DHS OneNet with an ISA, signed by the OneNet AO and by each applicable AO. Additional information regarding ISAs is published in Attachment N, *Preparation of Interconnection Security Agreements*, to the DHS 4300A *Sensitive Systems*	CA-3

Policy ID	DHS Policy Statements	Relevant Controls
	Handbook.	
5.4.3.d	ISAs shall be reissued every three (3) years or whenever any significant changes have been made to any of the interconnected systems.	CA-3
5.4.3.e	ISAs shall be reviewed and updated as needed as a part of the annual FISMA self-assessment.	CA-3
5.4.3.f	Components may complete a master ISA, (which includes all transitioning systems) as part of their initial OneNet transition. After transition, each additional system or GSS shall be required to have a separate ISA. Interconnections between DHS Components (not including DHS OneNet) shall require an ISA whenever there is a difference in the security categorizations for confidentiality, integrity, and availability between the systems or when the systems do not share the same security policies. (In this context, ‘security policies’ refers to the set of rules that controls a system’s working environment and not to DHS information security policy.) ISAs shall be signed by each applicable AO.	---
5.4.3.g	Components shall document interconnections between their own and external (Non-DHS) networks with an ISA for each connection.	CA-3
5.4.3.h	The DHS CIO shall approve all interconnections between DHS enterprise-level information systems and non-DHS information systems. 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.	CA-3
5.4.3.i	The Department and Components shall implement Trust Zones through Policy Enforcement Points (PEP), as defined in the DHS Security Architecture.	SC-7
5.4.3.j	DHS OneNet shall provide secure Name/Address resolution service. Domain Name System Security Extensions (DNSSEC) has been designated as the DHS service solution.	SC-20, SC-21, SC-22
5.4.3.k	All DHS systems connected to OneNet and operating at moderate or high level shall utilize secure Name/Address resolution service provided by DHS OneNet.	SC-20, SC-21, SC-22
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.	CM-3

Policy ID	DHS Policy Statements	Relevant Controls
5.4.3.m	Interconnections between two accredited DHS systems do not require an ISA if the interface characteristics, security requirements, nature of information communicated and monitoring procedures for verifying enforcement of security requirements are accounted for in the SPs or are described in another formal document, such as a Service Level Agreement (SLA) or contract, and the risks have been assessed and accepted by all involved AOs.	CA-3
5.4.3.n	Granting the ability to log into one DHS system through another DHS system (such as through OneNet trust) does not require an ISA, when the requirements from Section 5.4.3.m are met.	---

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 TICs and other approved direct system inter-connections. DHS TICs are provided by OneNet and monitored by the DHS EOC. Component SOCs may protect DHS-internal boundaries across Trust Zones.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.4.a	Components shall restrict physical access to firewalls and PEP to authorized personnel.	AC-4, SC-7
5.4.4.b	Components shall implement identification and strong authentication for administration of the firewalls and PEPs.	AC-4, SC-7
5.4.4.c	Components shall encrypt remote maintenance paths to the firewalls and PEPs.	MA-4, SC-7
5.4.4.d	Components shall conduct quarterly firewall and PEP testing to ensure that the most recent policy changes have been implemented and that *all* applied policies and controls are operating as intended.	SC-7
5.4.4.e	Component SOCs shall ensure that reports on information security operations status and incident reporting are provided to the DHS CISO as required.	IR-6
5.4.4.f	All Department and Component firewalls and PEPs shall be administered in coordination with DHS security operation capabilities, through the DHS EOC or Component SOCs.	SC-7
5.4.4.g	All DHS PEPs shall provide protection against denial-of-service attacks.	SC-5

Policy ID	DHS Policy Statements	Relevant Controls
5.4.4.h	Components shall determine protocols and services permitted through their Component-level PEPs. Components may restrict traffic sources and destinations at their Component-level PEPs.	SC-7
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 shall prevent traffic as directed by the DHS CIO.	SC-7
5.4.4.j	The DHS EOC shall oversee all enterprise PEPs.	---

5.4.5 Internet Security

Policy ID	DHS Policy Statements	Relevant Controls
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 TIC PEPs. The PSTN shall not be connected to OneNet at any time.	SC-7
5.4.5.b	Firewalls and PEPs shall be configured to prohibit any protocol or service that is not explicitly permitted.	CM-7, SC-7, SC-8, SC-9
5.4.5.c	Components shall ensure that all executable code, including mobile code (e.g., ActiveX, JavaScript), is reviewed and approved by the Program Manager prior to the code being allowed to execute within the DHS environment. [Note: When the technology becomes available and code can be vetted for security, the policy will be “Ensure that all approved code, including mobile code (e.g., ActiveX, JavaScript), is digitally signed by the designated DHS authority and that only signed code is allowed to execute on DHS systems.”]	SC-18
5.4.5.d	Telnet shall not be used to connect to any DHS computer. A connection protocol such as Secure Shell (SSH) that employs secure authentication (two factor, encrypted, key exchange) and is approved by the Component shall be used instead.	CM-7, SC-7, SC-8, SC-9
5.4.5.e	File Transfer Protocol (FTP) shall not be used to connect to or from any DHS computer. A connection protocol that employs secure authentication (two factor, encrypted, key exchange) and is approved by the Component shall be used instead.	CM-7, SC-7, SC-8, SC-9
5.4.5.f	Remote Desktop connections, such as Microsoft’s Remote Desktop Protocol (RDP), shall not be used to connect to or from any DHS computer without the use of an authentication method that employs secure authentication (two-factor, encrypted, key exchange).	AC-17, IA-2

Policy ID	DHS Policy Statements	Relevant Controls
5.4.5.g	In order to ensure the security and availability of DHS information and information systems, the DHS CIO or DHS CISO may direct that specific Internet websites or categories be blocked at the DHS TICs, on advice from US-CERT, the DHS EOC, or other reputable sources.	---

5.4.6 Email Security

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

DHS EOC personnel shall be trained to respond to incidents pertaining to email security and shall assist the email Steward as necessary. Components shall provide appropriate security for their email systems.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.6.a	Components shall correctly secure, install, and configure the underlying email operating system.	---
5.4.6.b	Components shall correctly secure, install, and configure mail server software.	---
5.4.6.c	Components shall secure and filter email content.	---
5.4.6.d	Components shall deploy appropriate network protection mechanisms, such as: - Firewalls - Routers - Switches - Intrusion detection systems	---
5.4.6.e	Components shall secure mail clients.	---
5.4.6.f	Components shall conduct mail server administration in a secure manner. This includes: - Performing regular backups - Performing periodic security testing - Updating and patching software - Reviewing audit logs at least weekly	---
5.4.6.g	The DHS email gateway Steward shall provide email monitoring for malware activity at the gateway.	SI-3
5.4.6.h	The DHS email gateway Steward shall provide email monitoring for spam at the gateway.	SI-8

Policy ID	DHS Policy Statements	Relevant Controls
5.4.6.i	Auto-forwarding or redirecting of DHS email to address outside of the .gov or .mil domain is prohibited and shall not be used. Users may manually forward individual messages after determining that the risk or consequences are low.	---
5.4.6.j	All DHS email systems are required to use the common naming convention with distinguishing identifiers for military officers, contractors, foreign nationals, and U.S. Government personnel from other Departments and agencies.	---

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.

5.4.7 Personal Email Accounts

Policy ID	DHS Policy Statements	Relevant Controls
5.4.7.a	The use of Internet webmail (Gmail, Yahoo, AOL) or other personal email accounts is not authorized over DHS furnished equipment or network connections.	---
5.4.7.b	When sending email to an address outside of the .gov or .mil domain, users shall ensure that any sensitive information, particularly PII, is attached as an encrypted file.	---

5.4.8 Testing and Vulnerability Management

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

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

Policy ID	DHS Policy Statements	Relevant Controls
5.4.8.a	Components shall conduct vulnerability assessments and/or testing to identify security vulnerabilities on information systems containing sensitive information annually or whenever significant changes are made to the information systems. This shall include scanning for unauthorized wireless	---

Policy ID	DHS Policy Statements	Relevant Controls
	devices. Evidence that annual assessments have been conducted shall be included in SARs and with annual security control assessments.	
5.4.8.b	Component CISOs/ISSMs shall approve and manage all activities relating to requests for Vulnerability Assessment Team (VAT) assistance in support of incidents, internal and external assessments, and on-going SLC support.	---
5.4.8.c	Component CISOs/ISSMs or their designated representatives shall acknowledge receipt of ISVM messages.	SI-5
5.4.8.d	Components shall report compliance with the ISVM message within the specified timeframe. Components unable to meet the designated compliance timeframe shall submit documentation of a waiver request via the DHS EOC Online Portal (https://eoconline.dhs.gov).	SI-5
5.4.8.e	When vulnerability assessment responsibilities encompass more than one Component, Component CISOs/ISSMs shall coordinate with the relevant Component SOC and the DHS EOC.	RA-3
5.4.8.f	The DHS EOC shall be notified before any ISVM scans are run.	RA-5
5.4.8.g	System Owners shall report the security alert and advisory status of the information system to the AO, Component CISO/ISSM, and DHS CISO upon request and on a periodic basis.	SI-5

5.4.9 Peer-to-Peer Technology

Policy ID	DHS Policy Statements	Relevant Controls
5.4.9.a	Peer to peer software technology is prohibited on any DHS information system.	CM-7, SA-6

5.5 Cryptography

Cryptography is a branch of mathematics that deals with the transformation of data. Transformation converts ordinary text (plaintext) into coded form (ciphertext) by encryption; and ciphertext into plaintext by decryption.

5.5.1 Encryption

Encryption is the process of changing plaintext into ciphertext for the purpose of security or privacy.

Policy ID	DHS Policy Statements	Relevant Controls
5.5.1.a	Systems requiring encryption shall comply with the following methods: Products using FIPS 197 Advanced Encryption Standard (AES) algorithms with at least 256 bit encryption that has been validated under FIPS 140-2, National Security Agency(NSA) Type 2, or Type 1 encryption. (Note: The use of triple Data Encryption Standard [3DES] and FIPS 140-1 is no longer permitted.)	IA-7, SC-13
5.5.1.b	Components shall develop and maintain encryption plans for sensitive information systems.	IA-7, SC-13
5.5.1.c	Components shall use only cryptographic modules that are FIPS 197 (AES-256) compliant and have received FIPS 140-2 validation at the level appropriate to their use.	IA-7, SC-13

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.)

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.a	The DHS CISO shall be the DHS PKI Policy Authority (PKI PA) to provide PKI policy oversight. A detailed description of DHS PKI PA roles and responsibilities are provided in the DHS PKI Policy.	SC-17
5.5.2.b	The DHS CISO shall represent DHS on the Federal PKI Policy Authority (FPKI PA.)	SC-17
5.5.2.c	The DHS PKI PA shall appoint a PKI Management Authority (PKI MA) to provide management and operational oversight of the DHS PKI. A detailed description of DHS PKI MA roles and responsibilities are provided in the DHS PKI Policy.	SC-17
5.5.2.d	The DHS PKI shall be governed by the U.S. Common Policy Framework certificate policy approved by the FPKI PA, and the DHS PKI Policy approved by the DHS PKI PA.	SC-17
5.5.2.e	DHS shall have a single DHS Principal CA that is subordinate to the U.S. Common Policy Root CA. The DHS Principal CA shall be operated for DHS by the Department of Treasury (DoT) under the Federal Shared Service Provider (SSP) program.	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.f	All additional CAs within DHS must be subordinate to the DHS Principal CA. The requirements and process for becoming a subordinate CA to the DHS Principal CA shall be specified in the DHS PKI Policy.	SC-17
5.5.2.g	Components that implement a CA shall ensure that the CA is subordinate to the DHS Principal CA.	SC-13
5.5.2.h	All DHS CAs shall have a trust path resolving to the U.S. Common Policy Root CA. The U.S. Common Policy Root CA is cross-certified with the Federal Bridge CA at the high, medium hardware, and medium assurance levels.	SC-17
5.5.2.i	The DHS Principal CA shall operate under an X.509 Certification Practices Statement (CPS). The CPS shall comply with the U.S. Common Policy Framework. DoT, as the SSP for DHS, approves the CPS for the DHS Principal CA.	SC-17
5.5.2.j	All DHS CAs subordinate to the DHS Principal CA shall operate under an X.509 CPS. The CPS shall comply with the U.S. Common Policy Framework and the DHS PKI Policy. The DHS PKI PA must approve the CPS.	SC-17
5.5.2.k	The DHS PKI PA shall ensure that the CPS for each subordinate DHS CA complies with the U.S. Common Policy Framework and DHS PKI Policy prior to approval.	SC-17
5.5.2.l	The DHS PKI MA shall ensure that every subordinate DHS CA operates in compliance with its approved CPS.	SC-17
5.5.2.m	All DHS CAs shall undergo regular PKI compliance audits as required by the U.S. Common Policy Framework and the DHS PKI Policy. The DHS PKI PA shall approve the auditor. The audit findings, report, and POA&Ms to address deficiencies found shall be provided to the DHS PKI PA and DHS PKI MA.	SC-17
5.5.2.n	All DHS CAs shall archive records as required by the U.S. Common Policy Framework and their CPS.	SC-17
5.5.2.o	All operational PKI facilities shall be established in accordance with U.S. Common Policy Framework physical security requirements based on the CA's assurance level and its intended use. Location/protection of the CA shall be determined by its level of assurance. Measures taken to ensure the continuity of PKI operations shall at least provide the same level of availability of PKI Services as the individual and composite availability requirements of the systems and data protected by the certificates.	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.p	The DHS Principal CA and DHS subordinate CAs shall only issue certificates to internal DHS entities, e.g., employees, contractors, roles, groups, applications, code signers, and devices. External entities who require certificates to securely interact with DHS shall acquire certificates from a non-DHS PKI that is cross-certified with the FBCA at medium assurance or above.	SC-17
5.5.2.q	Only the DHS Principal CA shall issue certificates to DHS employees, contractors, roles, code signers, and other human entities, including certificates for DHS HSPD-12 Personal Identify Verification (PIV) Cards. The DHS Principal CA may also issue all other types of certificates allowed under the U.S. Common Policy to internal DHS entities.	SC-17
5.5.2.r	DHS Subordinate CAs shall only issue certificates to internal non-human entities. Any additional restrictions on the types of certificates that may be issued by a specific subordinate DHS CA shall be determined during the subordination process and approved by the DHS PKI PA.	SC-17
5.5.2.s	The use by DHS of any non-DHS service provider for CA or PKI services is prohibited unless approved by the DHS CISO.	SC-13
5.5.2.t	Only certificates that are issued by the DHS Principal CA or a subordinate DHS CA under the U.S. Common Policy Framework at medium assurance or above shall be used to protect sensitive DHS data or to authenticate to operational systems containing sensitive data. Certificates issued by DHS CAs that are not established as subordinate to the DHS Principal CA, certificates issued by test, pilot, third party, self-signed or other CAs shall not be used to protect sensitive data, or to authenticate to DHS operational systems containing sensitive data.	SC-17

5.5.3 Public Key/Private Key

A public key certificate is used to obtain subscribers' public keys in a trusted manner. Once obtained, the public key is then 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

Policy ID	DHS Policy Statements	Relevant Controls
5.5.3.a	Separate public/private key pairs must be used for encryption and digital signature by human subscribers, organization subscribers, application subscribers, and code-signing subscribers.	SC-12
5.5.3.b	Separate public/private key pairs must be used for encryption and digital signature by device subscribers whenever supported by the protocols native to	SC-12

Policy ID	DHS Policy Statements	Relevant Controls
	the type of device.	
5.5.3.c	A human sponsor shall represent each application, role, code-signing, and device subscriber when it applies for one or more certificates from a DHS CA.	SC-12
5.5.3.d	An authorized DHS employee shall sponsor DHS contractors and other affiliates when they apply for one or more certificates from a DHS CA.	SC-12
5.5.3.e	A mechanism shall be provided for each DHS CA to enable PKI registrars to determine the eligibility of each proposed human, role, application, code signer, or device to receive one or more certificates.	SC-12
5.5.3.f	A mechanism shall be provided for each DHS CA to enable PKI registrars to determine and verify the identity of the authorized human sponsor for each DHS contractor, affiliate, role, application, code signer, or device.	SC-12
5.5.3.g	Human subscribers shall not share private keys and shall be responsible for their security and use. If a human subscriber discloses or shares his or her private key, the subscriber shall be accountable for all transactions signed with the subscriber's private key.	---
5.5.3.h	Sponsors for non-human subscribers (role, 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 Device Sponsor Agreement" as a pre-condition for sponsoring non-human subscribers.	SC-17
5.5.3.i	Subscriber private keys shall not be used by more than one entity, with the following exception. Multiple devices in a high availability configuration may use a single Secure Socket Layer (SSL) Subject Alternative Name (SAN) certificate, and thus use the same key pair.	SC-12
5.5.3.j	Every human subscriber shall read, understand, and sign a "DHS PKI Human Subscriber Agreement" as a pre-condition for receiving certificates from a DHS CA. These signed agreements shall be maintained by the DHS PKI MA.	SC-17

5.6 Malware Protection

Policy ID	DHS Policy Statements	Relevant Controls
5.6.a	Component CISOs/ISSMs shall establish and enforce Component-level malware protection control policies.	SI-3
5.6.b	Components shall implement a defense-in-depth strategy that: - Installs antivirus software on desktops and servers	SI-3

Policy ID	DHS Policy Statements	Relevant Controls
	- Configures antivirus software on desktops and servers to check all files, downloads, and email - Installs updates to antivirus software and signature files on desktops and servers in a timely and expeditious manner without requiring the end user to specifically request the update - Installs security patches to desktops and servers in a timely and expeditious manner	
5.6.c	System Owners shall develop and enforce procedures to ensure proper malware scanning of media prior to installation of primary hard drives, software with associated files, and other purchased products.	AC-20, SI-3

5.7 Product Assurance

Policy ID	DHS Policy Statements	Relevant Controls
5.7.a	Information Assurance (IA) shall be considered a requirement for all systems used to input, process, store, display, or transmit sensitive or national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated COTS IA and IA-enabled IT products. These products shall provide for the availability of systems. The products also shall ensure the integrity and confidentiality of information and the authentication and nonrepudiation of parties in electronic transactions.	---
5.7.b	*Strong preference* shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting sensitive information) that have been evaluated and validated, as appropriate, in accordance with the following: - The NIST FIPS validation program - The NSA/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program - The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement	---
5.7.c	The evaluation and validation of COTS IA and IA-enabled products shall be conducted by accredited commercial laboratories or by NIST.	---
5.7.d	Components shall use only cryptographic modules that meet the requirements set forth in Section 5.5, Cryptography.	---
5.7.e	Transaction-based systems (e.g., database management systems, transaction processing systems) shall implement transaction rollback and transaction	---

Policy ID	DHS Policy Statements	Relevant Controls
	journaling, or technical equivalents.	

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 1.7, 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 INFOSEC@dhs.gov.

APPENDIX A ACRONYMS

AC	Access Control
AES	Advanced Encryption Standards
AO	Authorizing Official
ARB	Acquisition Review Board
AT	Awareness and Training
ATO	Authority to Operate
AU	Audit and Accountability
BI	Background Investigation
BIA	Business Impact Assessment
BLSR	Baseline Security Requirements
CA	Certificate Authority Certification, Accreditation, and Security Assessments
CCB	Change Control Board
CFO	Chief Financial Officer
CI	Counter-Intelligence
C-I-A	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CISID	Chief, Internal Security and Investigations Division
CISO	Chief Information Security Officer
CM	Configuration Management
CMG	Core Management Group
CMP	Configuration Management Plan
CO	Certifying Official
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

CPIC	Capital Planning and Investment Control
CPS	Certificate Practices Statement
CRE	Computer-Readable Extract
CRL	Certificate Revocation List
CSIRC	Computer Security Incident Response Center
CSO	Chief Security Officer
CUI	Control Unclassified Information
DES	Digital Encryption Standards
DHS	Department of Homeland Security
DNSSEC	Domain Name System Security Extensions
DoD	Department of Defense
DoS	Department of State
DoT	Department of Treasury
EA	Enterprise Architecture
EAB	Enterprise Architecture Board
EO	Executive Order
EOC	Enterprise Operations Center
FBCA	Federal Bridge Certification Authority
FDCC	Federal Desktop Core Configuration
FICAM	Federal Identity, Credentialing, and Access Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOUO	For Official Use Only
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
IA	Identification and Authentication Information Assurance
IATO	Interim Authority to Operate
ICAM	Identity, Credentialing, and Access Management
IDS	Intrusion Detection System
IR	Incident Response Infrared
IRB	Investment Review Board
ISA	Interconnection Security Agreement
ISO	Information Security Office
ISSO	Information System Security Officer
ISVM	Information System Vulnerability Management
JWICS	Joint Worldwide Intelligence Communications System
IT	Information Technology
LAN	Local Area Network
LE	Law Enforcement
LMR	Land Mobile Radio
MA	Maintenance Major Application
MBI	Minimum Background Investigation
MD	Management Directive
MMS	Multimedia Messaging Service
MP	Media Protection
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NSA	National Security Agency
OCIO	Office of the Chief Information Officer

OID	Object identifier
OIG	Office of Inspector General
OIS	Office of Information Security
OMB	Office of Management and Budget
OPA	Office of Public Affairs
OPM	Office of Personnel Management
OTAR	Over-The-Air-Rekeying
PA	Policy Authority
PBX	Private Branch Exchange
PCS	Personal Communications Services
PDA	Personal Digital Assistant
PE	Physical and Environmental Protection
PED	Portable Electronic Device
PEP	Policy Enforcement Point
PHI	Protected Health Information
PIRT	Privacy Incident Response Team
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identity Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PKI PA	PKI Policy Authority
PKI PM	PKI Management Authority
PL	Planning
PM	Program Manager Program Management
PNS	Protected Network Services
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPOC	Privacy Point of Contact
PS	Personnel Security

PSTN	Public Switched Telephone Network
PTA	Privacy Threshold Analysis
RA	Risk Assessment Registration Authority
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFID	Radio Frequency Identification
RMS	Risk Management System
SA	Security Architecture System and Services Acquisition
SAN	Subject Alternative Name
SAR	Security Assessment Report
SAISO	Senior Agency Information Security Officer
SAOP	Senior Agency Official for Privacy
SC	System and Communications Protection
SCI	Sensitive Compartmented Information
SELC	Systems Engineering Life Cycle
SI	System and Information Integrity
SLA	Service Level Agreement
SMS	Short Message Service
SOC	Security Operations Center
SOP	Standard Operating Procedure
SORN	System of Records Notice
SP	Special Publication Security Plan
SSH	Secure Shell
SSL	Secure Socket Layer
SSP	Shared Service Provider
TAF	TrustedAgent FISMA
TFPAP	Trust Framework Provider Adoption Process
TIC	Trusted Internet Connections

TOS	Terms of Service
TRM	Technical Reference Model
TS	Top Secret
US-CERT	United States Computer Emergency Readiness Team
VA	Vulnerability Assessment
VAT	Vulnerability Assessment Team
USGBC	U.S. Government Configuration Baseline
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
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 NIST IR 7298, *Glossary of Key Information Security Terms* and the National Information Assurance (IA) Glossary.

Acceptable Risk	Mission, organizational, or program-level risk deemed tolerable by the RE after adequate security has been provided.
Accreditation Package	The documents submitted to the AO for the Accreditation Decision. An Accreditation Package consists of: Accreditation 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
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	DHS activity for meeting the annual FISMA self-assessment requirement.
Authorizing Official (AO)	An official within a Federal Government agency who can grant approval for a system to operate.
Cellular phone	A mobile device used for voice communication irrespective of the communications technology employed.
Certification/ Certifying Agent	A contractor that performs certification tasks as designated by the CO.
Certifying Authority (CA)	Obsolete term; see Security Control Assessor
Security Control Assessor	A senior management official who certifies the results of the security assessment. He or she must be a Federal Government employee.
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 all DHS offices 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).
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.
Enterprise Operations Center (EOC)	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	The marking instruction or caveat “For Official Use Only” will be used to identify sensitive but unclassifed information within the DHS community 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)	DHS system that provides notification of newly discovered vulnerabilities and tracks the status of vulnerability resolution.
Information System Security Officer (ISSO)	Someone 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 resulting 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 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 Statement	A high-level rule for guiding actions intended to achieve security objectives.
Policy Enforcement Point (PEP)	A firewall or similar device that can be used to restrict information flow.
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.
Production	Operational, as in "production system" or "production environment."
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 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 DHS Component organization that coordinates security operations within its Component.
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.
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 or alien number (A-number).
Significant Incident	A computer security-related incident that represents a meaningful threat to the DHS mission and requires immediate leadership notification.
Spam	E-mails 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 accreditation boundary.

System Owner	??
Technical Controls	The security controls for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware elements of the system.
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 by its USB plug.
USB Drive	A memory device small enough to fit into a pocket and that connects to a computer by its USB plug.
Vulnerability Scanning	An automated scan for potential security vulnerabilities.
Waiver	Acceptance to temporarily operate a system that does not comply with policy while working towards 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. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, DC, July 14, 1987
- Public Law 107-347, *E-Government Act* of 2002, including Title III, *Federal Information Security Management Act (FISMA)*
- Public Law 104-106, *Clinger-Cohen Act* of 1996 [formerly, Information Technology Management Reform Act (ITMRA)]
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*
- Public Law 100-235, *Computer Security Act* of 1987 as amended
- Public Law 93-579, *Freedom of Information Act* of 2002 as amended

Executive Orders

- Executive Order 13526, *Classified National Security Information*, December 29, 2009
- 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*
- OMB Bulletin 06-03, *Audit Requirements for Federal Financial Statements*
- 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*
  - NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
- 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)
  - NIST SP 800-34, Rev 1, *Contingency Planning Guide for Information Technology Systems*
  - NIST SP 800-37, Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
  - NIST SP 800-39, *Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View* (Draft)
  - NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
  - NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*
  - NIST SP 800-53, Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*
  - NIST SP 800-53A, Rev 1, *Guide for Assessing the Security Controls in Federal Information Systems*
  - NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*
  - NIST SP 800-63, Rev 1, *Electronic Authentication Guideline* (Draft)
  - NIST SP 800- 65, Rev 1, *Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process (CPIC) (Draft)*

- NIST SP 800-88, *Guidelines for Media Sanitization*
- NIST SP 800-92, *Guide to Computer Security Log Management*
- NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*
- NIST SP 800-95, *Guide to Secure Web Services*
- NIST SP 800-100, *Information Security Handbook: A Guide for Manager*
- NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*
- NIST SP 800-118, *Guide to Enterprise Password Management* (Draft)
- *NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
- NIST SP 800-123, *Guide to General Server Security*
- NIST SP 800-124, *Guidelines on Cell Phone and PDA Security*
- NIST SP 800-128, *Guide for Security Configuration Management of Information Systems* (Draft)
- NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (Draft)

- NIST IR 7298, *Glossary of Key Information Security Terms*
- CNSS Instruction No. 4009, *National Information Assurance Glossary*
- CNSS Instruction No. 1001, *National Instruction on Classified Information Spillage*

Internal Guidance

- Department of Homeland Security Acquisition Regulation (HSAR)
- DHS Management Directives (MD), especially:
    - MD 140-01, *Information Technology Systems Security*
    - MD 11042.1, *Safeguarding Sensitive but Unclassified (For Official Use Only) Information*
    - MD 102-01 *Acquisition Management*
    - MD 1030, *Corrective Action Plans*
    - MD 4400.1, *DHS Web and Information Systems*
    - MD 4500.1, *DHS Email Usage*
    - MD 4600.1, *Personal Use of Government Office Equipment*
    - MD 4900, *Individual Use and Operation of DHS Information Systems/Computers*
    - MD 11055, *Suitability Screening Requirements for Contractor Employees*

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, 4.6.2.d, 4.6.3.f, 5.2.c, 5.4.8.a, 5.6.b. New sections: 4.1.1. Modified

Version	Date	Description
		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 forty-five (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 14, 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. “IT Security Program” changed to “Information Security Program”

Version	Date	Description
		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) and Computer Security Incident Response Center (CSIRC).”

Version	Date	Description
		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. 4.9 – Section was renamed "Department Information Security Operations." 4.9, 4.9.1, 4.9.2 – Updated policy elements to support Department security

Version	Date	Description
		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. **Section 1.0** 1.2 – Added reference to E-Government Act of 2002, January 7, 2003.

Version	Date	Description
		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. 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.

Version	Date	Description
		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	July 31, 2009	**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 Added Appendix A – Acronyms

Version	Date	Description
		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:

Version	Date	Description
		2.1.3.b - All Components shall be responsible to the appropriate CISO. 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 3.7 – 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 3.11.1 – 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 (due to adding of privacy section 3.14.5

Version	Date	Description
		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) **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 outsource this capability to the DHS SOC. The DHS SOC shall provide

Version	Date	Description
		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. 5.5.3.g – Sponsors for non-human subscribers (organization, application,

Version	Date	Description
		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 or .mil addresses. 5.4.6.i **-** Auto-forwarding or redirecting of DHS email to address outside of the .gov or .mil domain is prohibited and shall not be used. Users may manually forward individual messages after determining that the risk or consequences are low. **Section 5.4.7 – Personal Email Accounts** – Requires use of encryption when sending sensitive information to email addresses other than .gov or .mil addresses. 5.4.7.b **-** When sending email to an address outside of the .gov or .mil domain, users shall ensure that any sensitive information, particularly privacy data, is attached as an encrypted file. **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 4.6.2 and 5.4.1.a** – Prohibits tethering to DHS devices

Version	Date	Description
		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	May 17, 2010	**General Updates** 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 and link to CPIC Guide **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 HIPAA information **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 both AOs must accept risk for interconnected systems that do not require ISAs. **Section 5.4.3.m-n** – Adds stipulations to ISA requirements

Version	Date	Description
		Section 5.5 – Updates language in entire section **Section 5.5.3.j** – Assigns the DHS PKI MA responsibility for maintaining Human Subscriber agreements
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 **Section 1.4.1/3** – Updates Executive Order reference from 12958 to 13526 **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

Version	Date	Description
		personnel **Section 4.12.i** – Updates escort requirements for maintenance or disposal **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 **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.
8.0	March 14, 2011	**General Updates** Update date and version number 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 “system security plan” with “security plan” and “SSP” with “SP”. **Specific Updates** **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 1.6.d:** Added new policy element, “DHS and Component systems shall be able to verify PIV credentials issued by other Federal agencies.” **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 eternal providers who operate information systems meet the same security requirements as the Component. **Section 2.1.4:** Update list of Component ISSM duties and create a POA&M

Version	Date	Description
		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 2.2.8:** Add Program Manager responsibility for POA&M content. **Section 2.2.9:** Add expanded System Owner duties. **Section 2.2.11:** Renumber 2.2.10 as 2.2.11. **Section 2.2.10:** Add a new 2.2.10 to introduce and describe duties of Common Control Provider. **Section 3.2.g:** Added new policy element, "Procurements for services and 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 3.10.b:** Policy element language was updated to clarify the function of information system security review and assistance programs. **Section 3.14:** Language updated for readability. **Section 3.14.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 4.1.4.d:** Language updated to clarify usage of administrator accounts. **Section 4.1.5.f:** Language updated to clarify requirements for security awareness training plan. **Section 4.3.1.b:** Language updated to clarify protection of offsite backup media. **Section 4.5.4:** Added reference to NIST SP 800-58 for more information on VoIP.

Version	Date	Description
		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 4.10:** Revise list of annual system documentation updates. **Section 4.12.c:** Policy element replaced with new one stating that the policy 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 5.4.1.e:** Policy element removed. **Section 5.4.1.f:** Policy element removed. **Appendix A:** Include new acronyms **Appendix B:** Revise definition of Accreditation Package to reflect new list of documentation. **Appendix C:** Update references