



DHS Sensitive Systems Policy Directive 4300A

INFORMATION TECHNOLOGY SECURITY PROGRAM

Version 5.5

September 30, 2007

This implements
DHS Management Directive 4300.1

DEPARTMENT OF HOMELAND SECURITY

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;

Version	Date	Description
		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 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, <i>Sensitive But Unclassified to For Official Use Only</i>
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	<p>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.</p> <p>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."</p> <p>Section 3.0: 3.9 – Inserted new policy element "I" regarding CISO concurrence for accreditation. 3.15 – Added text regarding Component CFOs and ISSMs.</p>

Version	Date	Description
		<p>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.</p> <p>Section 5.0: 5.1c – Changed inactive accounts to “disable user identifiers after 45 days of inactivity.” 5.1.1 – First sentence of the second paragraph was rewritten to prohibit use of personal passwords by multiple individuals. 5.2.2 – Title changed to “Automatic Session Termination.”</p>

TABLE OF CONTENTS

1.0	INTRODUCTION.....	1
1.1	IT Security Program Policy	1
1.2	Authorities.....	1
1.3	Policy Overview.....	2
1.4	Definitions.....	3
1.4.1	Classified National Security Information	3
1.4.2	National Security Information	3
1.4.3	Sensitive Information.....	3
1.4.4	Public Information	3
1.4.5	Information Technology (IT).....	3
1.4.6	DHS IT System.....	4
1.4.6.1	General Support System (GSS).....	4
1.4.6.2	Major Application (MA)	4
1.4.7	Component.....	4
1.4.8	Trust Domain	4
1.4.9	Operational Data.....	4
1.5	Waivers and Exceptions.....	4
1.6	Information Sharing and Communication Strategy	5
2.0	ROLES AND RESPONSIBILITIES.....	6
2.1	Secretary of Homeland Security	6
2.2	Under Secretaries and Heads of DHS Components.....	6
2.3	DHS Chief Information Officer (CIO)	6
2.4	Component Chief Information Officers.....	7
2.5	Chief Information Security Officer (CISO).....	8
2.6	Office of the Chief Privacy Officer (CPO).....	8
2.7	DHS Chief Security Officer (CSO)	9
2.8	Component Information Systems Security Manager (ISSM).....	9
2.9	Component Privacy Offices and Privacy Points of Contact (PPOC)	10
2.10	Program Managers (PM).....	11
2.11	United States Computer Emergency Readiness Team (US-CERT)	11
2.12	Certifying Official.....	11
2.13	Designated Accrediting Authority (DAA).....	12
2.14	Information Systems Security Officer (ISSO).....	12
2.15	System Owners	13
2.16	Users of DHS Supplied Computing Resources	13
2.17	Additional Personnel.....	14
2.18	DHS Chief Financial Officer designated Financial Systems	14
2.18.1	DHS CFO.....	14
2.18.2	DHS CIO.....	15
2.18.3	Component CFO	15
2.18.4	Component CIO	16
2.18.5	System Owners	17
3.0	MANAGEMENT POLICIES	18
3.1	Basic Requirements	18

3.2	Capital Planning and Investment Control	18
3.3	Contractors and Outsourced Operations	19
3.4	Performance Measures and Metrics.....	19
3.5	Continuity Planning for Critical DHS Assets	19
	3.5.1 Continuity of Operations Planning (COOP).....	20
	3.5.2 IT Contingency Planning (CP).....	20
3.6	System Development Life Cycle	21
3.7	Configuration Management	21
3.8	Risk Management	22
3.9	Certification and Accreditation, Remediation, and Reporting.....	22
3.10	IT Security Review and Assistance	24
3.11	Security Working Groups and Forums	24
	3.11.1 DHS Information Systems Security Board.....	24
	3.11.2 DHS IT Security Training Working Group	24
	3.11.3 DHS Wireless Security Working Group (WSWG)	25
3.12	IT Security Policy Violation and Disciplinary Action.....	25
3.13	Required Reporting.....	26
3.14	Privacy and Data Security.....	26
	3.14.1 Personally Identifiable Information (PII).....	26
	3.14.2 Privacy Impact Assessments.....	27
	3.14.3 Privacy Incident Reporting	27
	3.14.4 E-Authentication	28
3.15	DHS Chief Financial Officer Designated Financial Systems	28
4.0	OPERATIONAL POLICIES.....	31
4.1	Personnel.....	31
	4.1.1 Citizenship, Personnel Screening, and Position Categorization	31
	4.1.2 Rules of Behavior	31
	4.1.3 Access to Sensitive Information	31
	4.1.4 Separation of Duties.....	32
	4.1.5 IT Security Awareness, Training, and Education	32
	4.1.6 Separation from Duty.....	33
4.2	IT Physical Security.....	33
	4.2.1 General Physical Access	33
	4.2.2 Sensitive Facility.....	33
4.3	Media Controls.....	34
	4.3.1 Media Protection.....	34
	4.3.2 Media Marking.....	34
	4.3.3 Media Sanitization and Disposal	34
	4.3.4 Production, Input/Output Controls	34
4.4	Voice Communications Security	35
	4.4.1 Private Branch Exchange.....	35
	4.4.2 Telephone Communications	35
	4.4.3 Voice Mail	35
4.5	Data Communications.....	35
	4.5.1 Telecommunications Protection Techniques	35
	4.5.2 Facsimiles	35

4.5.3	Video Conferencing.....	35
4.5.4	Voice over Data Networks.....	36
4.6	Wireless Communications	36
4.6.1	Wireless Systems	37
4.6.2	Wireless Portable Electronic Devices (PED).....	38
4.6.2.1	Cellular Phones.....	39
4.6.2.2	Pagers	39
4.6.2.3	Multifunctional Wireless Devices	39
4.6.3	Wireless Tactical Systems	39
4.6.4	Radio Frequency Identification (RFID).....	40
4.7	Overseas Communications.....	41
4.8	Equipment	41
4.8.1	Workstations	41
4.8.2	Laptop Computers and Other Mobile Computing Devices	41
4.8.3	Personally Owned Equipment and Software (Not owned by or contracted for by the Government).....	41
4.8.4	Hardware and Software.....	42
4.8.5	Personal Use of Government Office Equipment and DHS IT Systems/Computers.....	42
4.8.6	Wireless Settings for Peripheral Equipment.....	43
4.9	Security Incidents and Incident Response and Reporting.....	43
4.9.1	Law Enforcement Incident Response	44
4.10	Documentation (Manuals, Network Diagrams).....	44
4.11	Information and Data Backup.....	45
4.12	Converging Technologies	45
5.0	TECHNICAL POLICIES	46
5.1	Identification and Authentication	46
5.1.1	Passwords.....	46
5.2	Access Control	47
5.2.1	Automatic Account Lockout.....	47
5.2.2	Automatic Session Termination.....	47
5.2.3	Warning Banner	47
5.3	Auditing	48
5.4	Network and Communications Security	48
5.4.1	Remote Access and Dial-In	48
5.4.2	Network Security Monitoring.....	49
5.4.3	Network Connectivity.....	49
5.4.4	Firewalls.....	50
5.4.5	Internet Security.....	50
5.4.6	Email Security.....	51
5.4.7	Personal Email Accounts	51
5.4.8	Testing and Vulnerability Management.....	51
5.4.9	Peer-to-Peer Technology	52
5.5	Cryptography	52
5.5.1	Encryption.....	53
5.5.2	Public Key Infrastructure.....	53

5.5.3 Public Key/Private Key.....54
5.6 Virus Protection56
5.7 Product Assurance56
6.0 DOCUMENT CHANGE REQUESTS.....57
7.0 QUESTIONS AND COMMENTS.....57

1.0 INTRODUCTION

This document articulates the Department of Homeland Security (DHS) Information Technology (IT) 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 IT security programs. The baseline security requirements (BLSRs) included in the handbook must be addressed when developing IT security documents.

1.1 IT Security Program Policy

The DHS IT 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 IT infrastructure and operations.

The policies and direction contained in this document apply to all DHS Components. IT security policies and implementing procedures for National Security Systems are covered in DHS National Security Systems Policy Directive 4300B and DHS 4300B National Security Systems Handbook.

The DHS IT Security Program does not apply to systems that process, store, or transmit National Intelligence Information.

Policy elements are effective when issued. Any policy elements that have not been implemented within 90 days shall be considered a weakness. Either a system or program POA&M must be generated by the Component for the identified weaknesses. When DHS Security Compliance tools (RMS and TAF) are required to be updated to reflect policy element changes, tool changes shall be available to the Department within 45 days of the policy changes.

1.2 Authorities

The DHS has established a Department-wide IT security program and organization based on the following Executive orders, public laws, and national policy:

- Federal Information Security Management Act (FISMA) of 2002, November 25, 2002
- Federal Financial Management Improvement Act of 1996 (FFMIA), P.L. 104-208
- Federal Managers' Financial Integrity Act of 1982 (FMFIA), P.L. 97-255
- The National Security Act of 1947, dated July 26, 1947
- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987
- Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996
- Public Law 107-296, Homeland Security Act of 2002

- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch
- Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, dated April 3, 1984
- Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities*, dated November 18, 1988, as amended
- Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*
- OMB Circular A123, *Management's Responsibility for Internal Control*, Revised, December 21, 2004
- OMB Circular A-127, *Financial Management Systems*, Revised December 1, 2004
- OMB Bulletin 06-03, *Audit Requirements for Federal Financial Statements* August 23, 2006
- Department of Homeland Security Acquisition Regulation (HSAR), June 2006
- DHS Management Directives (e.g., MD 0470.1, MD 1030, MD 4400.1, MD 4500.1, MD 4600.1, MD 11042.1, MD 11050.2)
- National Institute of Standards and Technology (NIST) Special Publications (e.g., 800-16, 800-34, 800-37, 800-50, 800-53) and Federal Information Processing Standards (FIPS) (e.g., FIPS 199, 200)
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000

1.3 Policy Overview

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

- **Management Controls** – Focus on managing both the IT security system and system risk. These controls consist of risk mitigation techniques and concerns normally addressed by management.
- **Operational Controls** – Focus on mechanisms primarily implemented and executed by people. These controls are designed to improve the security of a particular system, or group of systems. These controls require technical or specialized expertise and often rely on management and technical controls.
- **Technical Controls** – Focus on security controls executed by IT 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 InfoSec Glossary (http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf).

1.4.1 Classified National Security Information

Information that has been determined, pursuant to Executive Order 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status.

1.4.2 National Security Information

Information that has been determined, pursuant to Executive Order 12958 (as amended) or any predecessor order, to require protection against unauthorized disclosure.

1.4.3 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. This type of information concerning financial systems will be identified as Sensitive Financial Information, if on another system it would be identified as system vulnerability 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.

1.4.4 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)

1.4.5 Information Technology (IT)

The Clinger-Cohen Act defines information technology 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.

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

1.4.6 DHS IT System

A DHS system is any IT 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. DHS systems include general support systems and major applications.

1.4.6.1 General Support System (GSS)

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, applications, data and users. Examples of a GSS include a local area network (LAN), an agencywide backbone, a communications network, a data processing center, a tactical radio network, or a shared information processing service organization.

1.4.6.2 Major Application (MA)

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” An MA is distinguishable from a GSS by the fact that it is a discrete application, whereas a GSS may support multiple applications.

1.4.7 Component

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

1.4.8 Trust Domain

A Trust Domain 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 Domain may be set up between different network segments that require specific usage policies based on information processed, such as law enforcement information.)

1.4.9 Operational Data

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

1.5 Waivers and Exceptions

Components may request waivers to, or exceptions from, any portion of this policy, for up to 6 (six) months, whenever they are unable to fully comply with policy requirements. Requests are made, through the Information Systems Security Board (ISSB), to the Chief Information Security Officer (CISO) and shall include the operational justification, risk acceptance, risk mitigation measures, and a plan for bringing the system into compliance. A second waiver request for up to 6 (six) months may be made only by the Head of the Component and only if the waiver is reported as a material weakness in the Component’s Federal Information Systems Management Act (FISMA) report.

¹ OMB Circular A-130

A Component may request an Exception to Policy whenever it is unable to bring the system into compliance. Exceptions are generally limited to mission-specific systems that are not part of the DHS Enterprise Infrastructure. This request is made, through the ISSB, to the CISO and shall include the operational justification, risk acceptance, and risk mitigation measures.

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

NOTE: Special procedures apply for exception to the requirement that persons accessing DHS systems be U.S. Citizens (policy 4.1e). Under normal conditions, 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 Chief Information Officer. Attachment J to the DHS 4300A Sensitive Systems Handbook provides an electronic form for requesting exceptions to the U.S. Citizenship requirement.

1.6 Information Sharing and Communication Strategy

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

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

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

- Entering incident information into the DHS SOC incident database
- Generating preformatted incident reports
- Initiating queries of the incident database
- Viewing FISMA incident reporting numbers
- Automating portions of the Information Security Vulnerability Management (ISVM) program
- Automating portions of the vulnerability assessment program

2.0 ROLES AND RESPONSIBILITIES

Persons and organizations must understand their roles and responsibilities and adhere to all relevant Federal and Departmental regulations and guidance.

Designated personnel play a major role in the planning and implementation of IT security requirements. 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. The following presents a list of roles and responsibilities for implementing these requirements.

2.1 Secretary of Homeland Security

The Secretary of Homeland Security is responsible for ensuring that DHS IT systems and their data are protected in accordance with Congressional and Presidential directives. To that end, the Secretary:

- Ensures the integrity, confidentiality, availability, authenticity, and nonrepudiation of information and information systems.
- Ensures that DHS implements its IT Security Program throughout the life cycle of each DHS system.
- Submits (1) the Chief Information Officer's assessment of the adequacy and effectiveness of the Department's information security procedures, practices, and FISMA compliance, and (2) the results of an independent information security program evaluation performed by the DHS Inspector General, annually to the Director of the Office of Management and Budget (OMB)

2.2 Under Secretaries and Heads of DHS Components

The Under Secretaries and the heads of DHS Components:

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

2.3 DHS Chief Information Officer (CIO)

The DHS Chief Information Officer (CIO) will establish and oversee the Department-wide IT Security Program, ensure proper computer security incident response, and provide consulting assistance to all DHS offices for their individual programs. The DHS CIO provides management

direction for the DHS Security Operations Center (SOC) and overall direction for Component SOCs. The DHS CIO, or designated representative, has the sole responsibility for public release of information concerning computer security incidents. The CIO will consult with the DHS Privacy Office and Public Affairs Office prior to releasing any information.

The DHS CIO:

- Appoints a Federal employee in writing to serve as the DHS Chief Information Security Officer (CISO).
- Serves as the Designated Accrediting Authority (DAA) for DHS enterprise IT 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 IT systems acquisition documents, including existing contracts, include appropriate IT security requirements and comply with DHS IT 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 IT Security Program annually.
- Ensures that an IT security performance metrics program is developed, implemented, and funded.
- Reports to the Under Secretary for Management on matters relating to the security of DHS IT systems.

2.4 Component Chief Information Officers

Component CIOs provide management direction to their security operations and are the principal advocates for computer security incident response.

Component Chief Information Officers (CIO):

- Establish and oversee their Component IT security programs.
- Ensure that a Component Information System Security Manager (ISSM) has been appointed.
- Ensure that a Designated Accrediting Authority (DAA) has been appointed for all Component IT systems and serve as the DAA for any IT system where a DAA has not been appointed or where a vacancy exists.
- Ensure that IT security concerns are addressed by Component Configuration Control Boards, Architecture Review Board, and Investment Review Board.
- Ensure that an accurate IT systems inventory is established and maintained.
- Ensure that an IT 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 SOC within reporting time requirements as defined in Attachment F 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.*

2.5 Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) reports directly to the CIO, serves as the Department-wide Information Systems Security Manager (ISSM), and is the principal advisor for IT security matters.

The CISO:

- Issues Department-wide IT security policy, guidance, and architecture requirements for all DHS IT systems and networks
- Implements and manages the Department-wide IT Security Program and ensure compliance with FISMA and OMB requirements.
- Serves as the principal Departmental liaison with organizations outside the DHS for matters relating to IT security.
- Reviews and approves the tools, techniques, and methodologies planned for use in certifying and accrediting DHS IT systems. This includes Security Test and Evaluation (ST&E) plans, contingency plans, and risk assessments.
- Reviews requests for waivers and exception to DHS IT security policy.
- Consults with the DHS Chief Security Officer on matters pertaining to physical security, personnel security, information security, investigations, and SCI systems, as they relate to IT security and infrastructure.
- Briefs the DHS CIO and senior management on the status and outcome of ongoing and completed computer security incidents.
- Tests and evaluates periodically the effectiveness of information security policies, procedures, and practices.
- Develops and implements procedures for detecting, reporting, and responding to computer security incidents.
- Ensures preparation and maintenance of plans and procedures to provide continuity of operations for information systems.

2.6 Office of the Chief Privacy Officer (CPO)

The Chief Privacy Officer (CPO) is responsible for Departmental compliance with privacy policy, including measures for securing information security assets and activities. The CPO works to maintain privacy requirements, while supporting security requirements.

The CPO serves as the senior official responsible for:

- Oversight of privacy incident management
- Responding to suspected or confirmed privacy incidents or incidents involving Personally Identifiable Information (PII)
- Coordinating with the DHS CIO and senior management when dealing with high-impact privacy incidents
- Providing the status and outcomes of ongoing and completed privacy incidents
- Distributing reports to the DHS and Component CIOs
- Receiving reports that impact DHS privacy programs
- Working with the DHS CIO and DHS CISO in preparation for release of computer security incident information involving PII or other privacy issues
- Convening and chairing incident response teams, such as the Privacy Incident Response Team (PIRT) and the Core Management Group (CMG)

2.7 DHS Chief Security Officer (CSO)

The Chief Security Officer (CSO) reports directly to the Deputy Secretary on all matters pertaining to security within the DHS. Pursuant to Executive Order 12958, as amended, the CSO is designated the Senior Agency Official. In that capacity, the CSO:

- Directs and administers the Department's program under which information is classified, safeguarded, and declassified.
- Coordinates the Department's classification management program and serve as the DHS point of contact with the Information Security Oversight Office.
- Provides support and coordinates with the Department's emergency planning and response efforts and activities.
- Provides guidance and oversight on meeting physical security requirements.

2.8 Component Information Systems Security Manager (ISSM)

The Information Systems Security Manager (ISSM) are the principal interface between the Office of the CISO, Component Information Systems Security Officers (ISSOs) and other security practitioners. As such, the ISSM plays a critical role in ensuring that the DHS IT Security Program is implemented and maintained throughout the Component. The ISSM must be a DHS employee and must be appointed by the appropriate Component executive.

ISSMs:

- Oversee the Component IT security program.
- Ensure that IT security-related decisions and information, including updates to the 4300 series of IT security publications, are distributed to the ISSOs and other appropriate persons within their Component.
- Ensure that the Component CIO is kept apprised of all pertinent matters involving the security of IT systems.
- Approve and/or validate all Component IT system security reporting.

- Consult with the Component Privacy Office or Privacy Point of Contact (PPOC) for reporting and handling of privacy incidents.
- Manage IT security resources including oversight and review of Exhibit 300 funding documents.
- Review and approve the security of hardware and software prior to implementation into the Component SOC.
- Test the security of implemented systems
- Implement and manage the Plan of Action and Milestones (POA&M) process.
- Maintain an inventory of all IT systems.
- Ensure the Component IT security program is structured to support DHS and appropriate FISMA and OMB requirements.
- Develop and publish procedures necessary to implement the requirements of DHS IT security policy within the appropriate Component.
- Ensure that Information Systems Security Officers (ISSO) are appointed for each IT system managed at the Component level.
- Review and approve ISSO appointments.
- Ensure that the CISO-approved Risk Management System (RMS) automated tool is utilized for conducting certification and accreditation evaluations.
- Ensure that the CISO-approved Trusted Agent FISMA (TAF) automated tool is utilized for conducting self-assessment evaluations and for reporting required IT security program status information.
- Ensure that weekly incident reports are submitted to the DHS SOC.
- Acknowledge receipt of Information Security Vulnerability Management (ISVM) messages, report compliance with requirements or notify the granting of waivers.

2.9 Component Privacy Offices and Privacy Points of Contact (PPOC)

The Component Privacy Offices and Privacy Points of Contact (PPOC) are responsible for compliance with Federal laws and DHS privacy policy at the Component level. The Privacy Officers and PPOCs work with the Component CIO and DHS CPO to maintain privacy requirements. SOCs will work with their Component Privacy Offices, PPOCs, or with the DHS CPO to address suspected or confirmed privacy incidents (PI) or incidents involving PII.

Component Privacy Offices and Privacy Points of Contact:

- Advise the Component CIO and management regarding privacy issues relevant to the Component.
- Receive and evaluate reports that impact DHS privacy programs.
- Work with system owners to complete privacy impact assessments
- Coordinate with program managers, Component ISSMs, CSIRC, or SOC in evaluating and reporting suspected or confirmed incidents involving PII.

- Inform the DHS CPO of the status of ongoing and completed privacy incidents in a timely manner.
- Advise the CPO regarding the handling of reported privacy Incidents.
- Provide privacy incident updates to US-CERT as further information is obtained.
- Work with the DHS CPO, Component CIO and Component CISO in preparation for release of computer security incident information involving PII or other privacy issues
- Work with the Component CIO and DHS Privacy Officer in preparation for release of computer security incident information involving PII or other privacy issues

2.10 Program Managers (PM)

Program Managers are responsible for ensuring compliance with applicable Federal laws, directives and Departmental policy governing the security, operation, maintenance and privacy protection of IT systems, information and programs under his or her control.

Program Managers:

- Work with system owners, Component ISSMs, and their staffs to ensure information systems are properly secured.
- Understand how to recognize and respond to suspected or confirmed security incidents, privacy incidents or incidents involving PII.
- Consult with Component privacy offices or PPOCs concerning privacy incidents and other privacy issues affecting IT systems and programs under his or her control.
- Prepare and transmit written Privacy Event Notification (PEN) simultaneously to Component privacy offices/PPOCs, the Component CIO and ISSM.
- Supplement privacy incidents reports to the DHS SOC and US-CERT as information becomes available.

2.11 United States Computer Emergency Readiness Team (US-CERT)

The United States Computer Emergency Readiness Team (US-CERT) is designated as the central reporting organization within the Federal Government and serves as the central repository for Federal incident data. The DHS SOC will report security incidents to the US-CERT. The US-CERT may notify law enforcement, the Identity Theft Task Force, the Social Security Administration, and the Executive Office of the President, as appropriate.

2.12 Certifying Official

A Certifying Official (typically the ISSM) is assigned to each IT system by an appropriate Component official. A Certifying Official may be responsible for more than one system.

Certifying Officials must be Federal employees and must be designated in writing for each IT system. Designation letters shall be signed by the appropriate Under Secretary or Component Head. The Certifying Official:

- Ensures that required Certification and Accreditation (C&A) activities are completed, and that the test results are documented.

- Ensures that a risk analysis is performed and that it identifies risks, determines their magnitude, and identifies areas needing safeguards.
- Ensures that a system test and evaluation is conducted and the results of such tests are documented or updated annually.
- Ensures that rules of behavior and security procedures/guides are developed.
- Ensures that a contingency plan is prepared and tested annually
- Ensures that the C&A documentation is recorded in the DHS C&A Tool and FISMA Reporting Tool
- Reviews the C&A package (SSP, Security Assessment Report, and POA&M) and recommends to the DAA whether or not the system should be accredited.
- Prepares the security accreditation decision letter for the DAA's signature.

2.13 Designated Accrediting Authority (DAA)

The Designated Accrediting Authority (DAA) controls personnel, operations, maintenance, and budgets for the systems or field site and has the authority to formally assume responsibility for operating an IT system at an acceptable level of risk. The DAA should control the resources necessary to mitigate risks.

A DAA shall be assigned to each IT system and may be responsible for more than one system. The DAA should be the system owner or an appropriate program official. (i.e., A Component CFO would be assigned as the DAA for a CFO designated financial system) The Component CIO shall serve as DAA anytime the system owner or an appropriate program official cannot be named.

DAAs:

- Review Notices of Findings and Recommendations (NFR) and Plans of Action and Milestones (POA&M)
- Review and approve corrective actions necessary to mitigate residual risks.
- Approve/disapprove system accreditation, or issue an Interim Authorization to Operate (IATOs may be issued only for systems in development testing or for prototypes).
- Terminate system operation if security conditions warrant such action.

2.14 Information Systems Security Officer (ISSO)

An Information Systems Security Officer (ISSO) shall be appointed in writing, by the appropriate official, for each IT system. An ISSO may either be a Federal employee or an appropriately cleared support contractor and may be assigned to more than one system. For financial or privacy systems, ISSOs shall not be assigned collateral duties.

ISSOs:

- Serve as the principal points of contact for all IT security aspects pertaining to their systems.
- Work closely with the Component ISSM and DHS CISO staff to interpret and apply IT security policies and implementing procedures.

- Serve as liaison between system owners and the ISSM.
- Work with system owners to document weaknesses in POA&Ms and initiate corrective action.
- Employ automated tools (approved by the DHS CISO) such as the Risk Management System (RMS) and Trusted Agent FISMA (TAF).

2.15 System Owners

System owners use information technology to help achieve the mission needs within their program area of responsibility. As such, they are responsible for the successful operation of the IT systems within their program area and are ultimately accountable for the security of the IT systems and programs under their control.

System owners:

- Serve as the Designated Accrediting Authority (DAA) for systems under their purview
- Ensure that an ISSO is formally assigned to each IT system under their control and that this assignment is appropriately documented
- Ensure that required computer security functions and documentation are included in system life cycle planning and budgets
- Work closely with the CIO and other program and IT managers to ensure a complete understanding of risks, especially the increased risks resulting from interconnectivity with other programs and systems
- Document and manage accepted security risks in risk assessments
- Update the security of IT systems within their program area annually
- Ensure that system POA&Ms are prepared and maintained and that points of contact and resources are identified
- Prioritize security weaknesses for mitigation based on material weaknesses, external audits and program assessments
- Work with the Component Privacy Office or PPOC to Conduct Privacy Impact Assessments (PIA)
- Report Privacy and Computer Security incidents as appropriate, in coordination with the ISSM and Program Manager

2.16 Users of DHS Supplied Computing Resources

DHS employees, contractors, and vendors working on behalf of the DHS or its agencies, are responsible for reporting suspected or confirmed computer security incidents to their Component-level capability, or to the DHS SOC, in accordance with the Component's incident response procedures.

Successful situational awareness depends on effective security awareness and incident handling. Each Component will review its security awareness training requirements annually to ensure they reflect the evolving and changing nature of incidents.

2.17 Additional Personnel

Other personnel throughout DHS are responsible for various aspects of the IT security program. Contracting Officers and their Technical Representatives, project managers, system and network administrators, managers, supervisors, and users all play a role in helping to ensure the security of the Department's IT systems. The DHS 4300A Sensitive Systems Handbook provides a description of the roles and responsibilities of these additional personnel.

In implementing DHS IT security policy, Component heads will include these additional personnel in their security plans.

2.18 DHS Chief Financial Officer designated Financial Systems

The DHS CFO-designated financial systems require additional management accountability and effective internal control over financial reporting, as outlined in Section 3.15.

For CFO-designated financial systems, additional roles and responsibilities are summarized in this section.

2.18.1 DHS CFO

The Department CFO oversees application control definitions for financial systems as defined in OMB Bulletin No. 06-03, Audit Requirements for Federal Financial Statements, and DHS Technical Guidance No. 03-06–Laws and Regulations, Cross Servicing Assertion, and Draft OMB Bulletin 01-02. The Department CFO has committed to:

- Identifying financial systems subject to OMB A-123 and Internal Controls over Financial Reporting (ICOFR) requirements (“CFO-designated financial systems”).
- Working with the Department CIO to ensure the confidentiality, integrity and availability of financial data processing.
- Overseeing the development and establishment of policies and procedures regarding automated application controls for Department-wide application software processing financial data.
- Remediating automated application control deficiencies related to financial application policies and procedures at the Department level.
- Tracking and monitoring progress of automated application controls corrective action plans and remediation efforts at the Department and Component Levels.
- Working with the Department CIO to identify and incorporate user requirements for new financial applications or existing Departmental financial applications.
- Working with the DHS CIO to integrate and test the Department-wide business continuity plan.
- Coordinating with the DHS CIO to identify the financial data to be backed up and recovered and developing policies to ensure that procedures are in place for backing up and recovering critical financial data.

2.18.2 DHS CIO

The Department CIO is responsible for overseeing compliance of CFO-designated financial systems with Federal system security regulations and guidelines as documented in DHS Sensitive Systems Policy Directive 4300A, including support for OMB Circular A-123. The Department CIO:

- Ensures sufficient resources are provided to support the Department's compliance tracking.
- Reviews and evaluates the Department-wide IT Security Program.
- Categorizes information system deficiencies by OMB A-123 information technology general controls (ITGC) domains and TrustedAgent FISMA (TAF) risk levels.
- Remediates Information Technology General Control (ITGC) deficiencies related to policies and procedures at the Department level.
- Tracks and monitors progress of ITGC Plans of Action and Milestones (POA&M) and remediation efforts at the Department and Component levels.
- Ensures that Contracts and Interagency Agreements (IAA) include Homeland Security Acquisition Regulation (HSAR) security clauses.
- Develops Department-wide system development lifecycle methodology and monitor Component compliance with this methodology.
- As part of developing new financial applications or updating existing Departmental applications, integrates CFO feedback to ensure user requirements are adequately addressed.
- Develops and tests Department-wide disaster recovery plan. Coordinate with CFO to incorporate business continuity requirements and test on a periodic basis.
- Based on coordination with Department CFO, develops and implement Department-wide procedures for the routine backing up and recovering of financial data.

2.18.3 Component CFO

The Component CFO, working with the Component system owners, is responsible for overseeing implementation and compliance of IT controls for CFO-designated financial systems at the Component level. The Component CFO:

- Works with the Component CIO and owners of CFO-designated financial systems to help ensure the reliability of financial data processing through Component systems.
- Develops and establishes policies and procedures regarding automated application controls for software processing of financial data.
- Remediates automated application controls deficiencies at the Component level.
- Works with system owners to designate an Information System Security Officer (ISSO) for each of the CFO-designated financial systems, as defined in Section 3.15 of DHS Sensitive Systems Policy Directive 4300A.

- Tracks and monitors progress of automated application controls remediation efforts at the Component level.
- Works with system owners of CFO-designated financial systems to ensure remediation of ITGC deficiencies related to IT policies and procedures.
- Approves accreditation of enterprise CFO-designated financial systems, if not already identified as the Designated Accrediting Authority (DAA). In this role, accept security risk identified during audits of CFO-designated financial systems, on behalf of the Department.
- Works with Component CIO to incorporate user requirements for new financial applications or upgrades to existing financial applications.
- Works with Component CIO to integrate and test Component-wide business continuity plan.
- Coordinates with Component CIOs to identify the financial data needed to be backed up and recovered.

2.18.4 Component CIO

The Component CIO is responsible for overseeing implementation and compliance of CFO-designated financial systems at the Component level. The Component CIO:

- Reviews and evaluates the Component's CFO-designated financial systems to ensure ITGCs are in place and working effectively.
- Works with the system owners to ensure remediation of ITGC deficiencies related to CFO-designated financial systems.
- Tracks and monitors progress of ITGC POA&Ms and remediation efforts at the Component level.
- Ensures completion of Memorandums of Understanding (MOUs) and Interconnection Security Agreements (ISAs) for CFO-designated financial system interconnections with any system not owned by DHS; ensures that they include appropriate security clauses; and monitors service provider for compliance with MOUs and ISAs.
- Implements the Department-wide system development lifecycle methodology and monitor user compliance with this methodology.
- As part of developing new financial applications or updating existing applications, integrates CFO feedback to ensure user requirement are adequately addressed.
- Develops and tests Component-wide disaster recovery plan. Coordinate with Component CFO to incorporate business continuity requirements and test on a periodic basis.
- Based on Component CFO requirements, executes policies for the routine backing up and recovery of financial data. Implements policies and procedures for rotating back-up media off-site.

2.18.5 System Owners

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

- Work with Component ISSMs and their staffs to ensure CFO-designated financial systems are properly secured.
- Designate an ISSO as defined in Section 3.15, Directives 4300 and 4300A (draft).
- Ensure ITGCs are implemented and tested as required in DHS policy.
- Develop, implement, and test application controls, as appropriate.
- Ensure the completeness, accuracy, validity, and security of data inputs into, processed by, and output from the financial application.
- Ensure that Interconnection Security Agreements (ISA) are completed and enforced.
- Ensure that system POA&Ms are prepared and implemented with resources identified.
- Ensure resources are available for correcting weaknesses.
- Review and update the security of IT systems within their program area, in consultation with the Component CIO and ISSM, at least annually.
- Prioritize security weaknesses based on material weaknesses, external audits, and program assessments.
- Comply with Department system development life cycle methodology for new system implementations or modifications to existing systems.
- Participate in the developing and testing of disaster recovery plans for CFO-designated financial systems.

3.0 MANAGEMENT POLICIES

3.1 Basic Requirements

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

Component ISSMs will submit all security reports concerning DHS IT systems (major applications and general support systems) to the Component senior official or designated representative. ISSMs will interpret and manage DHS security policies and procedures to meet Federal, Departmental, and Component requirements. They will also answer data queries from the Compliance and Oversight Program Director and develop and manage information security guidance and procedures unique to Component requirements.

ISSOs are the primary points of contact for the IT systems assigned to them. They develop and maintain System Security Plans and are responsible for overall system security.

DHS Policy
a. Every DHS computing resource (e.g., desktops, laptops, servers, portable electronic devices) shall be individually accounted for as part of a recognized IT system.
b. The CIO, in cooperation with each Component senior official, shall be responsible for ensuring that every DHS computing resource is designated as a part of an IT system (major application or general support system).
c. A System Security Plan shall be prepared and accurately maintained for each DHS IT system.
d. An ISSO shall be designated for every DHS IT system.
e. Component IT Security Programs shall be structured to support DHS and applicable FISMA and OMB requirements.
f. IT security reports regarding DHS IT systems shall be submitted to the Component senior official or designated representative.
g. The ISSO for each IT system shall serve as the POC for all security matters related to that system.
h. ISSMs shall ensure that their IT systems comply with the DHS Enterprise Architecture (EA) and Security Architecture (SA) or maintain a waiver, approved by the DHS CIO/CISO.

3.2 Capital Planning and Investment Control

DHS Policy
a. System owners shall include IT security requirements in their capital planning and investment business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP).
b. System owners or DAAs shall ensure that IT security requirements and POA&Ms are adequately

DHS Policy
funded, resourced and documented in accordance with current OMB budgetary guidance.
c. Component Investment Review Boards (IRBs) shall not approve any capital investment in which the IT security requirements are not adequately defined and funded.

3.3 Contractors and Outsourced Operations

DHS Policy
a. All statements of work and contract vehicles shall identify and document the specific security requirements for IT services and operations required of the contractor.
b. Contractor IT services and operations must adhere to all DHS IT security policies.
c. Requirements shall address how sensitive information is to be handled and protected at the contractor's site, including any information stored, processed, or transmitted using the contractor's computer systems, the background investigation and/or clearances required, and the facility security required.
d. Statements of work and contracts shall require that at the end of the contract, the contractor must return all information and IT resources provided during the life of the contract and must certify that all DHS information has been purged from any contractor-owned system used to process DHS information.
e. Components shall conduct reviews to ensure that the IT security requirements are included within the contract language and are implemented and enforced.
f. Security deficiencies in any outsourced operation shall require creation of a program-level POA&M.

3.4 Performance Measures and Metrics

DHS Policy
a. Components shall define performance measures to evaluate the effectiveness of their IT security program.
b. Components shall provide quarterly and annual OMB FISMA data on their progress in implementing IT security performance measures.

3.5 Continuity Planning for Critical DHS Assets

The Continuity Planning for Critical DHS Assets Program is vital to the success of the DHS IT Security Program and consists of two integrated elements:

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

3.5.1 Continuity of Operations Planning (COOP)

DHS Policy
a. A standard DHS-wide process for continuity planning shall be developed, documented, and maintained in order to ensure continuity of operations under all circumstances
b. Components shall develop, test, implement, and maintain comprehensive COOPs to ensure the continuity and recovery of essential DHS functionality.
c. All COOPs shall be tested/exercised annually.
d. All CFO designated financial systems requiring high availability shall be identified in COOP plans and exercises.
e. All personnel involved in COOP efforts shall be identified and trained in the procedures and logistics of COOP development and implementation.

3.5.2 IT Contingency Planning (CP)

DHS Policy
a. Guidance, direction, and authority for IT contingency planning activities for all DHS Components are centralized in the DHS Office of the CIO.
b. To ensure critical IT system availability under all circumstances, a standard DHS-wide process for IT contingency planning shall be developed, documented, and maintained.
c. Components shall implement and enforce backup procedures for all sensitive IT systems, data, and information. Recommended intervals are daily for incremental data backups and weekly for full data backups. System and application software should be backed up whenever modifications to the software make backups necessary.
d. The rigor of the IT system contingency planning, training, testing and capabilities shall be dependent upon the FIPS 199 defined potential impact level. The availability security objective alone shall be applied to the NIST SP 800-53 contingency planning (CP) controls defined for the low, moderate, and high potential impact level systems.
e. Comprehensive IT Contingency Plans to continue and recover critical DHS major applications and general support systems shall be developed, tested, exercised, 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.
f. When testing is required, IT Contingency Plans shall be tested/exercised annually.
g. All personnel involved in IT contingency planning efforts shall be identified and trained in the procedures and logistics of IT contingency planning and implementation as required.
h. Personnel involved in IT contingency planning efforts shall receive IT Contingency Plan training or refresher training annually.

3.6 System Development Life Cycle

DHS Policy
a. Components shall ensure that system security is integrated into all phases of the System Development Life Cycle (SDLC).
b. Components shall ensure that security requirements for sensitive IT systems are incorporated into life-cycle documentation.
c. All custom developed code shall be reviewed, approved and signed by the Program Manager 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.

3.7 Configuration Management

Configuration management (CM) relates to managing the configuration of all hardware and software elements within IT 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 will apply to all systems, subsystems, and components of the DHS infrastructure, thereby ensuing implementation, and continuing life-cycle maintenance. CM begins with base lining of requirements documentation and ends with decommissioning of items no longer used for production or support.

The CM discipline will be applied to hardware, including power systems, software, firmware, documentation, test and support equipment, and spares. The Change Control Board (CCB) will ensure 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 IT system elements are consistent with the certification and accreditation 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 Policy
a. Components shall prepare configuration management plans for all IT systems, as part of their SSPs.
b. Components shall establish, implement, and enforce configuration management controls on all IT systems and networks and address significant deficiencies as part of a Plan of Action and Milestones (POA&M).
c. IT security patches must be installed in accordance with configuration management plans and within the timeframe or direction stated within the Information Security Vulnerability Management (ISVM)

DHS Policy
message published by the DHS SOC.

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 IT systems and data that support their organization's missions.

DHS Policy
a. Components shall establish a risk management program in accordance with National Institute of Standards and Technology Special Publication (NIST SP) 800-30, <i>Risk Management Guide for Information Technology Systems</i> .
b. Components shall conduct and document risk assessments every three years, when high impact weaknesses are identified, or whenever significant changes to the system configuration or to the operational/threat environment have been made, whichever occurs first.
c. Special rules apply to CFO designated financial systems. See Section 3.15 for additional information.

3.9 Certification and Accreditation, Remediation, and Reporting

FISMA directs that all Federal agencies develop and implement a Department-wide information system security program designed to safeguard IT assets and data. DHS bases its C&A policy on the recommendations set forth in NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, and OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

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

Accreditation is the official management decision by the DAA, that authorizes the operation of an IT system. It includes explicitly accepting the risk to agency operations, assets, or individuals, based on the implementation of an agreed-upon set of security controls. The DAA accepts security responsibility for the operation of certified IT systems and officially declares that a specified IT system is approved to operate (ATO) based on these protections. DAAs shall be identified in TrustedAgent FISMA (TAF). The Component CIO will serve as the DAA for any system in which another DAA has not been appointed.

DHS Policy
a. Components shall assign an impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability) and shall apply NIST 800-53 controls specific to the security objective at the determined impact level. Impact levels shall be assigned according to the

DHS Policy
standards set in FIPS Pub 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i> , and following the guidance from NIST SP 800-60, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i> . DHS C&A policy is based on guidance from NIST SP 800-37, <i>Guide for the Security Certification and Accreditation of Federal Information Systems</i> . [Note: See 4300A Sensitive Systems Handbook for information on the security objective(s) relevant to each of the NIST 800-53 controls.]
b. All Components shall implement NIST SP 800-53 security controls, using the FIPS Pub 200, <i>Minimum Security Requirements for Federal Information and Information Systems</i> methodology, based on the impact level established for each security objective (confidentiality, integrity, availability). A minimum impact level of “ moderate ,” shall be assigned and a risk-based assessment shall be performed to determine whether the confidentiality security objective warrants being assigned an impact level of “ high ,” for all CFO designated financial systems and for systems processing or hosting personally identifiable information (PII).
c. Components should pursue type C&A for IT 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 C&A will consist of a master C&A package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites.
d. The DAA for a system shall be identified in TrustedAgent FISMA. The Component CIO shall serve as the DAA when the system owner or an appropriate program official has not been named as the DAA.
e. Component ISSMs shall ensure that all new or major upgrades of existing sensitive IT systems and networks are formally certified through a comprehensive evaluation of their management, operational, and technical security features.
f. The certification, 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.
g. Component ISSMs shall ensure that a risk assessment is conducted whenever any modifications are made to sensitive IT systems, networks, or to their physical environments, interfaces, or user community. SSPs shall be updated and re-certification conducted if warranted.
h. Components shall accredit systems at initial operating capability and every 3 years thereafter, or whenever a major change occurs, whichever occurs first.
i. DAAs 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 must be certified and accredited in an Authorization to Operate (ATO) letter prior to passing the Key Decision Point 3 milestone in the development life cycle. IATOs are not appropriate for operational systems. The DAA may grant an IATO for a maximum period of 6 (six) months and may grant 1 (one) 6 (six) month extension.

DHS Policy
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.
k. As a result of IG auditing experience, components shall request concurrence from CISO for all accreditations for six months or less.
l. All DHS IT systems shall be accredited using the automated tools, TAF and RMS, approved by the DHS CISO.

3.10 IT Security Review and Assistance

DHS Policy
a. Components shall submit their IT security policies to the DHS CISO for review.
b. Components shall establish an IT Security Review and Assistance Program within their respective security organization.
c. Components shall conduct their reviews in accordance with FIPS 200/NIST SP 800-53, for specification of security controls. NIST SP 800-53A must be used for the assessment of security control effectiveness and for quarterly and annual FISMA reporting.
d. The DHS CISO shall conduct IT security review and assistance visits throughout the Department in order to monitor the Components' security program compliance with DHS policies and procedures.

3.11 Security Working Groups and Forums

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

3.11.1 DHS Information Systems Security Board

The DHS Information Systems Security Board (ISSB) consists of Component ISSMs and is chaired by the CISO. The ISSB is a decision-making body that considers a broad range of IT security matters of importance to the DHS IT Security Program.

DHS Policy
a. Component Information Systems Security Managers (ISSM) shall actively participate in the ISSB.
b. ISSMs shall ensure that the Component CIO is kept apprised of all pertinent matters involving the security of IT systems and that security-related decisions and information, including updates to the 4300 series of IT security publications, are distributed to the ISSOs and other appropriate persons.

3.11.2 DHS IT Security Training Working Group

The DHS IT Security Training Working Group is established to promote collaboration on IT security training efforts throughout the Department and to share information on Component-developed training activities, methods, and tools, thereby saving costs and avoiding duplication

of effort. The IT Security Training Working Group is chaired by the DHS Program Director for IT Security Training.

DHS Policy
a. Components shall appoint a representative to the DHS IT Security Training Working Group.
b. Each representative shall be responsible for managing the Component's IT security training program.
c. Component members shall actively participate in the DHS IT Security Training Working Group.

3.11.3 DHS Wireless Security Working Group (WSWG)

The DHS Wireless Security Working Group (WSWG) coordinates and evaluates DHS-wide approaches to wireless security on behalf of the Wireless Management Office (WMO) and the CISO. The WSWG focuses on policy, planning, and risk management; wireless security in major IT programs; and risk assessment of emerging technologies. The group assists the CIO in formulating and coordinating Department-wide security policies and guidelines related to wireless services and technologies.

DHS Policy
The DHS CIO and Components shall designate representatives to the DHS Wireless Security Working Group (WSWG).

3.12 IT Security Policy Violation and Disciplinary Action

Individual accountability is a cornerstone of an effective security policy. Component heads are responsible for taking corrective actions when security incidents and violations occur and for holding personnel accountable for intentional transgressions. Each Component must determine how to best address each individual case.

DHS Policy
a. IT security-related violations are addressed in the <i>Standards of Ethical Conduct for Employees of the Executive Branch</i> 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.
b. Non-DHS Federal employees or contractors who fail to comply with Department security policies are subject to having their access to DHS IT systems and facilities terminated, whether or not the failure results in criminal prosecution.
c. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions.

3.13 Required Reporting

The Federal Information Security Management Act (FISMA) requires that the status of the DHS IT Security Program be reported to the Office of Management and Budget (OMB) on a recurring basis.

DHS Policy
a. Components shall collect and submit quarterly and annual IT security program status data as required by FISMA.
b. Components shall utilize the automated tool approved for use by the DHS CISO.

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 DHS Privacy Office (privacy@dhs.gov; 571-227-3813). Please refer to the DHS Chief Privacy Officer web page for additional information.

Various regulations place restrictions on the Government's collection, use, maintenance, and release of information about individuals. Regulations also place requirements on agencies to protect PII, which is defined as information in a system or online collection that directly or indirectly identifies an individual (e.g., information about an individual's education, financial transactions, medical history, and criminal or employment history and information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number, date and place of birth, mother's maiden name, biometric records).

A Privacy Threshold Analysis (PTA) must be performed for IT systems to determine whether or not a full Privacy Impact Assessment (PIA) is required. The purpose of a PIA is to demonstrate that system owners and developers have consciously incorporated privacy protections throughout the system's lifecycle.

3.14.1 Personally Identifiable Information (PII)

OMB M-06-16 (Protection of Sensitive Agency Information) requires that agencies protect PII that is physically removed from the agency location or that is accessed remotely. Physical removal includes both removable media as well as media within mobile devices (i.e., laptop hard drive).

General policies relating to PII are provided below. Additional PII-related policies are included in the following sections of the DHS 4300A *Sensitive Systems Handbook*:

- Section 3.9: Certification and Accreditation, Remediation, and Reporting. For systems involving PII, 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.

- Section 5.2.2: Automatic Session Lockout. Sessions on workstations and on laptop computers and other mobile computing devices are to be terminated after 20 minutes of inactivity.
- Section 5.3: Auditing. Policies on audit logs of computer-readable extracts of personally identifiable information from databases and on erasure of these extracts are provided.
- Section 5.4.1: Remote Access and Dial-in. Remote access of PII must be approved by the DAA. Strong authentication via virtual private network (VPN) or equivalent encryption (e.g., https) and two-factor authentication is required. Restrictions are placed on the downloading and remote storage of PII accessed remotely.

DHS Policy
a. PII shall not be physically removed from a DHS facility without written authorization from the system DAA or person designated in writing by the DAA.
b. PII removed from a DHS facility shall be encrypted.
c. If PII can be physically removed from an IT system (printouts, CDs, etc), the System Security Plan shall document the specific procedures, training, and accountability measures in place to ensure remote use of the encrypted data does not bypass the protections provided by the encryption.

3.14.2 Privacy Impact Assessments

Privacy Impact Assessments (PIAs) are required whenever a new IT system is being developed or an existing system is significantly modified. PIAs are the responsibility of the System Owner and the IT Program Manager as part of the system development lifecycle process. OMB Memorandum M-03-22 and DHS MD 0470.1 discuss the requirements for conducting PIAs.

DHS Policy
Privacy Impact Assessments shall be conducted as part of new IT system development or whenever an existing system is significantly modified.

3.14.3 Privacy Incident Reporting

Reporting of privacy incidents and incidents that may involve PII are a special case, subject to strict reporting standards and timelines. These types of incidents are reported using the Privacy Event Notification (PEN).

DHS Policy
a. Any Component discovering a suspected or confirmed incident must coordinate with the Component Privacy Office or PPOC and ISSM in order to evaluate and subsequently report the incident to the DHS SOC.
b. The Component Privacy Officer or PPOC, in cooperation with the ISSM, shall jointly evaluate the incident, but the ISSM is responsible for reporting the incident to the Component CSIRC/SOC (or directly to the DHS CSIRC if the Component does not have its own SOC/CSIRC).

DHS Policy
<p>c. The ISSM shall report ALL types of privacy incidents, whether or not they involve IT resources. This unitary reporting process shall remain in effect until each Component has a Privacy Office or PPOC who can fulfill the reporting duties.</p>
<p>d. DHS personnel must 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.</p>

3.14.4 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 IT system must be evaluated to determine whether or not e-authentication requirements apply.

E-authentication guidance is provided in the following:

- OMB M-0404: E-Authentication Guidance for Federal Agencies, December 16, 2003
- NIST SP 800-63: Electronic Authentication Guideline, April 2006

DHS Policy
<p>a. Components shall determine whether or not Government e-authentication security requirements apply to their systems allowing online transactions.</p>
<p>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.</p>
<p>c. Components shall implement the technical requirements described in NIST SP 800-63, <i>Electronic Authentication Guideline</i>, at the appropriate assurance level for those systems for which e-authentication requirements apply.</p>

3.15 DHS Chief Financial Officer Designated Financial Systems

DHS CFO designated financial systems are systems that require additional management accountability and effective internal control over financial reporting. This section provides additional requirements for these systems based on OMB Circular A-123, *Management's Responsibility for Internal Control (A-123)* Appendix A. 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 financial systems, this section takes precedence.*

These additional requirements provide a strengthened assessment process and management assurance on the internal control over financial reporting. The strengthened process requires management to document the design and test the effectiveness of controls over financial reporting. The system owner is responsible for ensuring that all requirements, including security

requirements, are implemented on DHS systems. Component ISSMs must coordinate with their CFO organization to ensure that these requirements are implemented.

DHS Policy
a. System owners are responsible for ensuring that Security Test and Evaluation (ST&E) plans and security assessments of key security controls for CFO designated financial systems are completed annually. The assessment shall be performed during the first quarter of each fiscal year.
b. The DHS Chief Financial Officer (CFO) shall designate the financial systems that must comply with additional internal controls and the Office of the CFO shall review and publish this list during the fourth quarter of every fiscal year.
c. ISSMs shall ensure that semi-annual vulnerability assessments and verification of critical patch installations are conducted on all CFO designated financial systems. Vulnerability assessment shall be performed during the second quarter of each fiscal year.
d. All CFO designated financial systems shall be assigned a minimum impact level of “ moderate ” for confidentiality, integrity, and availability as described in Section 3.9.1 of the 4300A <i>Sensitive Systems Handbook</i> .
e. All security accreditations for CFO designated financial systems shall be approved and signed by the DAA <i>and</i> by the Component CFO.
f. System owners are responsible for ensuring that Disaster Recovery (DR) plans are created for <i>all</i> CFO designated financial systems requiring high availability and that each plan is tested annually, no later than the third quarter of each fiscal year.
g. ISSMs shall ensure that weekly incident response tracking is performed for all CFO designated financial systems.
h. ISSMs shall ensure that incidents related to CFO designated financial systems are reported to the Component CFO.
i. System owners are responsible for ensuring that risk assessments for all CFO designated financial systems are updated annually.
j. Financial application mission owners shall update CFO designated financial systems’ System Security Plans (SSP) annually. Key controls that address the relevant assertions for a material activity shall be identified in the SSP.
k. Component ISSMs must request a waiver from the DHS CISO if a key control weakness is identified for a CFO designated financial system and not remediated within 12 months.
l. Component CFOs shall ensure that a full-time dedicated ISSO is assigned to each CFO designated financial system. ISSOs should not be assigned collateral duties outside information security responsibilities. Designated financial system ISSOs may be assigned to more than one CFO designated financial system.

DHS Policy
<p>m. CFO designated financial system ATOs shall be rescinded if Components fail to comply with testing and reporting requirements established within this policy.</p>
<p>n. Component CFOs shall work with their Component ISSMs to approve any major system change to CFO designated financial system identified in the DHS inventory.</p>

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

DHS Policy
a. Components shall designate the position sensitivity level for all Government positions that use, develop, operate, or maintain IT systems and shall determine risk levels for each contractor position.
b. Components shall ensure the incumbents of these positions have favorably adjudicated background investigations commensurate with the defined position sensitivity levels.
c. No Federal employee shall be granted access to DHS systems without having a favorably adjudicated Minimum Background Investigation (MBI) as defined in DHS MD 11050.2, <i>Personnel Security and Suitability Program</i> .
d. No contractor personnel shall be granted access to DHS systems without having a favorably adjudicated Background Investigation (BI) as defined in DHS MD11055, <i>Suitability Screening Requirements for Contractor Employees</i> .
e. Only U.S. Citizens shall be granted access to DHS systems processing sensitive information. An exception to the U.S. Citizenship requirement may be granted by the Component senior official or designee with the concurrence of the Office of Security and the DHS CIO or their designees.

4.1.2 Rules of Behavior

DHS Policy
a. Components shall define rules of behavior for all IT systems and ensure that users are trained regarding these rules and are aware of the disciplinary actions that may result from violations.
b. Users shall sign rules of behavior prior to being granted IT accounts or access to any DHS IT systems or data.

4.1.3 Access to Sensitive Information

DHS Policy
System owners shall ensure that users of the IT systems supporting their programs have a valid requirement to access these systems.

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.

DHS Policy
Components shall divide and separate duties and responsibilities of critical IT 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.

4.1.5 IT Security Awareness, Training, and Education

DHS Policy
a. Components shall establish an appropriate IT Security Training Program for users of DHS systems.
b. DHS personnel and contractors accessing DHS IT systems shall receive initial training and annual refresher training, in security awareness and accepted security practices.
c. DHS personnel and contractors with significant security responsibilities (e.g., ISSOs, system administrators) shall receive initial specialized training, and annual refresher training thereafter, specific to their security responsibilities prior to being granted access to DHS IT systems.
d. Components shall maintain training records, to include name and position, type of training received, and costs of training. IT awareness training must be completed before IT accounts are authorized.
e. Unless a waiver is granted by the ISSM, user accounts and access privileges, including access to email, shall be disabled for those DHS employees who have not received annual refresher training.
f. Components shall prepare and submit an annual training plan, outlining their plans for IT Security Awareness, Training and Education. This plan shall follow the guidance in the DHS Component Information Technology (IT) Security Awareness, Training and Education Plan template, issued by the DHS IT Security Training Office.
g. Training plans shall include awareness of internal threats and basic IT security practices.
h. Components shall prepare and submit IT security Awareness, Training, and Education statistics to the DHS IT Security Training Program Director on a quarterly basis. These statistics shall include: <ul style="list-style-type: none"> – Total number of personnel and number of personnel that have received awareness. – Total number of personnel with significant security responsibility and the number that have received role-based training. – The cost of any agency-provided IT security training or materials for the year. Components must also provide: <ul style="list-style-type: none"> – Brief descriptions of the awareness and training provided to personnel. – Information concerning how they have explained policies relating to Peer-to-Peer (P2P) file sharing to all system users.
i. Components shall provide evidence of training by submitting copies of training schedules, training

DHS Policy

rosters, training reports, etc., upon request of the DHS IT Security Training Office, or during onsite validation visits performed on a periodic basis.

4.1.6 Separation from Duty

DHS Policy

a. Components shall implement procedures to ensure that system accesses are revoked for employees or contractors who leave the Component or are reassigned to other duties. Accounts for personnel on extended absences shall be temporarily suspended.
--

b. Components shall establish procedures to ensure that sensitive information stored on any media is transferred to an authorized individual upon termination or reassignment of an employee or contractor.
--

4.2 IT Physical Security

4.2.1 General Physical Access

DHS Policy

a. Access to DHS buildings, rooms, work areas, spaces, and structures housing IT systems, equipment, and data shall be limited to authorized personnel.
--

b. Controls for deterring, detecting, restricting, and regulating access to sensitive areas shall be in place and will be sufficient to safeguard against possible loss, theft, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters.

c. Controls shall be based on the level of classification and risk, determined in accordance with Departmental security policy.
--

d. Visitors must sign in upon entering DHS facilities, be escorted during their stay, and sign out upon leaving. Non-DHS contractors' access shall be limited to those work areas requiring their presence. Visitor logs shall be maintained and available for review for one year.
--

e. These requirements will extend to DHS assets, located at non-DHS facilities or non-DHS assets and equipment hosting DHS data.

4.2.2 Sensitive Facility

DHS Policy

a. Facilities processing, transmitting, or storing sensitive information shall incorporate physical protection measures based on the level of risk. The risk should be determined in accordance with Departmental security policy.

b. Any sensitive information or data not suitable for public dissemination shall be secured in one of the following: a locked office, room, desk, bookcase, file cabinet, or other storage prohibiting access by unauthorized persons.

4.3 Media Controls

4.3.1 Media Protection

DHS Policy
<p>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, or other storage prohibiting access by unauthorized persons) when not in use.</p>
<p>b. Components shall ensure that backup media are stored off site in accordance with their business continuity and IT Contingency plans.</p>
<p>c. DHS personnel and contractors 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.</p>
<p>d. All DHS USB drives must be compliant with FIPS 140-2 and FIPS 197</p>

4.3.2 Media Marking

DHS Policy
<p>Media determined by the information owner to contain sensitive information should be appropriately marked in accordance with DHS MD 11042.1: <i>Safeguarding Sensitive but Unclassified (For Official Use Only) Information</i>.</p>

4.3.3 Media Sanitization and Disposal

DHS Policy
<p>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.</p>
<p>b. Components shall maintain records of the sanitization and disposition of information systems storage media.</p>
<p>c. Components shall periodically test degaussing equipment to verify that the equipment is functioning properly.</p>

4.3.4 Production, Input/Output Controls

DHS Policy
<p>a. Components shall follow established procedures to ensure that sensitive information cannot be accessed or stolen by unauthorized individuals.</p>
<p>b. These procedures shall address not only the paper and electronic outputs from systems but also the transportation or mailing of sensitive media.</p>

4.4 Voice Communications Security

4.4.1 Private Branch Exchange

DHS Policy

Components shall provide adequate physical and IT 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.)

4.4.2 Telephone Communications

DHS Policy

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.

4.4.3 Voice Mail

DHS Policy

Sensitive information shall not be communicated over nor stored in voice mail.

4.5 Data Communications

4.5.1 Telecommunications Protection Techniques

DHS Policy

Components shall carefully select the telecommunications protection techniques that meet their security needs, in the most cost-effective manner, consistent with Departmental and Component IT policies. Approved guided media techniques or approved protected network services (PNS) may be used as cost-effective alternatives to the use of encryption for sensitive information requiring telecommunications protection.

4.5.2 Facsimiles

DHS Policy

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.

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.

4.5.3 Video Conferencing

DHS Policy

a. Components shall implement controls to ensure that only authorized individuals are able to

DHS Policy
participate in each videoconference.
b. Components shall ensure appropriate transmission protections, commensurate with the highest sensitivity of information to be discussed, are in place throughout any video teleconference.
c. Video teleconferencing equipment and software shall be disabled when not in use.

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.

DHS Policy
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 IT systems that employ this technology must be certified and accredited for this purpose with residual risks clearly identified in the Accreditation Package.
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.
c. Components shall ensure appropriate identification and authentication controls, audit logging, and integrity controls are implemented on every component of their voice over data networks.
d. Components shall ensure that physical access to voice over data network components is restricted to authorized personnel.

4.6 Wireless Communications

Wireless 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, IT 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).

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

DHS Policy
a. Wireless communications technologies are generally prohibited from use within DHS unless the appropriate DAA specifically approves a technology and application.
b. Components using 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.
c. The DHS WMO shall be notified within 30 days of all wireless communications systems acquisitions.

4.6.1 Wireless Systems

Wireless systems include wireless local area networks (WLAN), wireless wide area networks (WWAN), wireless personal area networks (WPAN), peer-to-peer wireless networks (i.e., ad hoc wireless networks), and IT systems that leverage commercial wireless services.

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

DHS Policy
a. Annual security assessments shall be conducted on all approved wireless systems. Wireless security assessments shall enumerate vulnerabilities, risk statements, risk levels, and corrective actions.
b. Risk mitigation plans shall be developed to address wireless security vulnerabilities. These plans shall prioritize corrective actions and implementation milestones in accordance with defined risk levels.
c. Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless system being approved for use.
d. System Security Plans 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 security solutions and secure connections to external interfaces are consistently enforced.
e. Legacy wireless systems that are not compliant with DHS IT 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 CISO, as appropriate.

4.6.2 Wireless Portable Electronic Devices (PED)

Wireless PEDs include 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, 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.

DHS Policy
a. The use of wireless PEDs and accessory devices in areas where sensitive or classified information is discussed is prohibited unless specifically authorized by the DAA in writing.
b. Wireless PEDs shall not be connected physically or wirelessly to the DHS-wired core network without written consent from the DAA.
c. Wireless PEDs shall not be used to store, process, or transmit combinations, personal identification numbers (PIN), or sensitive information in unencrypted formats.
d. Wireless PEDs such as BlackBerry devices and smartphones shall implement strong identification, authentication, data encryption, and transmission encryption technologies. Portable electronic devices such as BlackBerry devices and smartphones shall be password-protected, with a security timeout period established. For BlackBerry devices, the security timeout shall be set to 10 minutes.
e. System Security Plans shall promulgate the provisions, procedures, and restrictions for using wireless PEDs to download mobile code in an approved manner.
f. Wireless PEDs shall be operated only when current DHS Technical Reference Model (TRM)-approved versions of antivirus software and software patches are installed.
g. Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless PED being approved for use.
h. Components shall maintain a current inventory of all approved wireless PEDs in operation.
i. Wireless PEDs shall be cleared of all information before being reused by another individual, office, or Component within DHS or before they are surplus; wireless PEDs that are being disposed of, recycled, or returned to the owner or manufacturer shall first be sanitized using approved procedures.
j. Legacy wireless PEDs that are not compliant with DHS IT 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 CISO, as appropriate.
k. Personally owned PEDs shall not be used to process, store, or transmit sensitive DHS information.
l. The DAA shall approve the use of Government-owned PEDs to process, store, or transmit sensitive

DHS Policy
information.
m. The use of add-on devices such as cameras and recorders is not authorized unless approved by the DAA. Functions that can record or transmit sensitive information via video, IR, or RF shall be disabled in areas where sensitive information is discussed.

4.6.2.1 Cellular Phones

DHS Policy
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 and the DHS Wireless Management Office. Under no circumstances shall classified information be discussed on cellular phones.

4.6.2.2 Pagers

DHS Policy
Pagers shall not be used to transmit sensitive information.

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, etc). Most of these functions have no security.

DHS Policy
a. Functions that cannot be encrypted using approved cryptographic modules shall not be used to process, store, or transmit sensitive information.
b. Functions that transmit or receive video, infrared (IR), or radio frequency (RF) signals shall be disabled in areas where sensitive information is discussed.
c. Short Message Service (SMS) and Multimedia Messaging Service (MMS) shall not be used and shall be disabled whenever possible.

4.6.3 Wireless Tactical Systems

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

Wireless tactical system policy and procedures are described more completely in Attachment Q3 (*Wireless Tactical Systems*) to the DHS 4300A Sensitive Systems Handbook.

DHS Policy
a. DAAs shall be immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents.
b. Wireless tactical systems shall implement strong identification, authentication, and encryption.
c. Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless tactical system being approved for use.
d. Components shall maintain a current inventory of all approved wireless tactical systems in operation.
e. Legacy tactical wireless systems that are not compliant with DHS IT 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 CISO, as appropriate.
f. The security configuration of Land Mobile Radio (LMR) subscriber units shall be validated via over-the-air-rekeying (OTAR) or hard rekey using a crypto-period no longer than 180 days.
g. All LMR systems shall comply with Project 25 (P25, EIA/TIA-102) security standards where applicable.

4.6.4 Radio Frequency Identification (RFID)

Radio Frequency Identification allows 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 (*Sensitive RFID Systems*) to the DHS 4300A Sensitive Systems Handbook.

DHS Policy
a. Components implementing RFID systems shall assess hazards of electromagnetic radiation to fuel, ordinance, and personnel before deployment of the RFID technology.
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.
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.
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

DHS Policy

outside the Component's physical perimeter.

e. When the RFID system is connected to a DHS data network, Components shall implement network security controls to appropriately segregate RFID network components such as RFID readers, middleware, and databases from other non-RFID network hosts.

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.

4.7 Overseas Communications**DHS Policy**

Where required or appropriate, all overseas communications 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****DHS Policy**

a. Components shall ensure that all unattended workstations are either logged off, locked, or use a password-protected screensaver, activated after 5 minutes of inactivity.

b. Components shall ensure that workstations are protected from theft.

4.8.2 Laptop Computers and Other Mobile Computing Devices**DHS Policy**

a. Information stored on any laptop computer or other mobile computing device that may be used in a residence or on travel shall be encrypted using FIPS 140-2-approved encryption. Passwords and smart cards shall not be stored on or with the laptop or other mobile computing device.

b. 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.

c. Employees shall obtain the written approval of the office director before taking a laptop computer or other mobile computing device overseas.

4.8.3 Personally Owned Equipment and Software (Not owned by or contracted for by the Government)**DHS Policy**

a. Personally owned equipment and software shall not be used to process, access, or store sensitive information without the written prior approval of the Designated Accrediting Authority (DAA).

DHS Policy

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 ISSM.

4.8.4 Hardware and Software**DHS Policy**

a. Components shall ensure that the installation of hardware and software products meets the requirements specified in applicable DHS secure baseline configuration guides.

b. Components shall limit access to system software and hardware to authorized personnel.

c. Components shall test, authorize, and approve all new and revised software and hardware prior to implementation in accordance with their Configuration Management Plan.

d. Components shall manage systems to reduce vulnerabilities through vulnerability testing, promptly installing patches, and eliminating or disabling unnecessary services, if possible.

e. Maintenance ports shall be disabled and shall only be enabled during maintenance.

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

a. DHS employees may use Government office equipment and DHS IT 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*.

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 or cause degradation of network services. DHS users must comply with the provisions of DHS MD 4500, *DHS Email Usage*, and DHS MD 4400.1, *DHS Web and Information Systems*.

c. DHS users do not have any right to or expectation of privacy while using Government office equipment and/or DHS IT systems/computers, including Internet and email services.

d. The use of Government office equipment and DHS IT 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.

e. DHS users are required to sign rules of behavior prior to being granted IT accounts or access to DHS IT 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.

f. Contractors or other non-DHS employees are not authorized to use Government office equipment or IT systems/computers for personal use, unless limited personal use is specifically permitted by the

DHS Policy

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, etc) 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.

DHS Policy

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.
--

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 <i>and</i> obtain a waiver or exception in accordance with Section 1.5, Exceptions and Waivers.

4.9 Security Incidents and Incident Response and Reporting

The DHS SOC is currently the central coordinating and reporting authority for all "For Official Use Only" (FOUO) information, Component SOC's and computer security incidents throughout the Department. The HSDN SOC is the central coordinating and reporting authority for all SECRET computer security incidents throughout the Department. The DHS SOC works closely with the HSDN SOC, the DHS Office of Intelligence and Analysis (DHS I&A) and the DHS Chief Security Officer to coordinate security operations.

DHS Policy

a. Components shall establish and maintain a Component incident response capability.

b. Components shall report <i>significant incidents</i> to the DHS SOC as soon as possible via phone (703-921-6505) but not later than one hour from "validation," e.g. a security event being confirmed as a security incident. Other means of communication, such as the SOC portal (https://soconline.dhs.gov) (Accessible only via the DHS Intranet), are acceptable, but the Component is responsible for <u>positively verifying</u> that the notification is received and acknowledged by the DHS SOC.
--

c. Significant HSDN incidents shall be documented with a preliminary report that will be provided to the HSDN GWO or DHS CSIRC within one hour. An initial report detail will be provided to DHS CSIRC within four hours. Subsequent updates and status reports will be provided to DHS CSIRC every 24 hours until incident resolution or when new information is discovered. Significant incidents are reported individually on a per incident basis and will not be reported in the monthly summary report. Refer to DHS 4300A Attachment H Section 2.6 for guidance.
--

d. Components shall report minor incidents on systems in the weekly incident report. SBU systems

DHS Policy
may report via the DHS SOC portal (https://soconline.dhs.gov) (Accessible only via the DHS Intranet). Components with no portal access will report minor incidents via email to dhs.soc@dhs.gov . HSDN incidents will be documented in a summary report provided to the HSDN GWO or DHS CSIRC on a weekly basis
e. All reports must be classified at the highest classification level of the information contained in the document. Unsanitized reports are marked and handled appropriately. Refer to MD4300A Attachment F for guidance.
f. If a DHS Component has no incidents to report for a given week, a weekly “No Incidents” report shall be sent via the DHS SOC portal (https://soconline.dhs.gov) (Accessible only via the DHS Intranet). Components with no portal access will report minor incidents via email sent to dhs.soc@dhs.gov .
g. The DHS CSIRC shall report incidents to US-CERT, in accordance with the DHS SOC CONOPS, as they arrive. Components should not send incident reports directly to US-CERT.

4.9.1 Law Enforcement Incident Response

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

DHS Policy
a. Components shall coordinate all external law enforcement involvement through the DHS SOC. Exceptions are only made during emergencies where time is critical to saving lives or protecting property. In cases of emergency notification, the Component will notify the DHS SOC as soon as possible, by the most expedient means available.
b. Components should obtain guidance from the DHS SOC before contacting local law enforcement.

4.10 Documentation (Manuals, Network Diagrams)

DHS Policy
a. Components shall ensure that IT systems and networks are appropriately documented in such a way as to allow others to understand system operation and configuration.
b. Documentation shall be updated whenever system changes occur.
c. Documentation shall be kept on hand and be accessible to authorized personnel (including DHS auditors) at all times.
d. System documentation may be categorized as FOUO if deemed appropriate by the ISSM. This category shall not be used as a means to restrict access to auditors or other personnel.

4.11 Information and Data Backup

DHS Policy
Components shall implement and enforce backup procedures as part of their contingency planning.

4.12 Converging Technologies

Advances in technology have resulted in the availability of devices that offer multiple functions. Many devices such as multifunctional desktop computers, copiers, fax machines, and heating, ventilation and air conditioning (HVAC) systems may contain sensitive data and may also be connected to data communications networks.

DHS Policy
<p>a. The policies in this document, including C&A requirements, apply to any devices that process or host DHS data,</p>
<p>b. Component ISSMs shall determine whether or not automated process devices should be included as part of an IT system's C&A requirements.</p>

5.0 TECHNICAL POLICIES

The design of IT 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 IT systems is individually accountable for his or her actions while utilizing the system.

5.1 Identification and Authentication

DHS Policy
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.
b. For IT systems requiring authentication controls, the IT system shall ensure that each user is authenticated before IT system access occurs.
c. For systems with low impact for the confidentiality security objective, Components shall disable user identifiers after 90 days of inactivity; for systems with moderate and high impacts for the confidentiality security objective, Components shall disable user identifiers after 45 days of inactivity.
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.
e. All user authentication materials shall be treated as sensitive material and shall carry a level as high as the most sensitive data to which that user is granted access using that authenticator.

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.

DHS Policy
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.
b. The ISSO shall determine and enforce the appropriate frequency for changing passwords but in no case shall the frequency be less often than every 180 days.
c. DHS users shall not share personal passwords.
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 must be approved by the appropriate DAA.
e. Scripted passwords shall not be used.

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

DHS Policy
a. Components shall implement access control measures that provide protection from unauthorized alteration, loss, unavailability, or disclosure of information.
b. Access control shall follow the principles of least privilege and separation of duties and shall require users to use unique identifiers. <i>Social Security Numbers shall not be used as login IDs.</i>
c. Users shall not provide their passwords to anyone, including system administrators.
d. Emergency and temporary access authorization shall be strictly controlled and must be approved by the ISSM prior to being granted.

5.2.1 Automatic Account Lockout

Components shall configure each IT system to lock a user's account for a specified period following a specified number of consecutive failed logon attempts.

DHS Policy
a. Components shall implement and enforce an account lockout policy that limits the number of consecutive failed logon attempts to three.
b. Components shall configure systems to lock a user's account for 20 minutes after three consecutive failed logon attempts.

5.2.2 Automatic Session Termination

Components shall configure each IT system to deactivate any user session immediately and automatically following a specified period of inactivity, in such a way that will require the user to re-authenticate his identity before resuming interaction with the system.

DHS Policy
Components shall ensure that sessions on workstations, laptops, and PEDs are terminated after 20 minutes of inactivity.

5.2.3 Warning Banner

DHS Policy
a. IT systems internal to the DHS network shall display a warning banner stipulated by the DHS CISO.
b. IT systems accessible to the public shall provide both a security and privacy statement at every

DHS Policy
entry point.

5.3 Auditing

DHS Policy
<p>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 IT System Security Plan. The audit record shall contain at least the following information:</p> <ul style="list-style-type: none"> – Identity of each user and device accessing or attempting to access an IT system – Time and date of the access and the logoff – Activities that might modify, bypass, or negate IT security safeguards – Security-relevant actions associated with processing. – All activities performed using an administrator's identity.
<p>b. Audit records for financial systems or for systems hosting or processing PII shall be reviewed by the system administrator monthly. Unusual activity or unexplained access attempts shall be reported to the system owner and ISSM.</p>
<p>c. Components shall ensure that their audit records and audit logs are protected from unauthorized modification, access, or destruction.</p>
<p>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 90 days.</p>
<p>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 SSP.</p>
<p>f. Computer-readable data extracts involving PII shall be erased within 90 days unless the information included in the extracts is required beyond the 90 days. Erasure of the extracts or the need for continued use of the data shall be documented by the Component Privacy Officer or PPOC.</p>

5.4 Network and Communications Security**5.4.1 Remote Access and Dial-In**

DHS Policy
<p>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 ISSM.</p>
<p>b. Components shall ensure that remote access and approved dial-in capabilities provide strong</p>

DHS Policy
authentication and access control and audit and protect sensitive information throughout transmission. In addition, remote access solutions shall comply with the encryption requirements of FIPS 140-2, <i>Security Requirements for Cryptographic Modules</i> . Dial-up connections shall be centrally managed by each Component to ensure integrity of network security. Strong authentication for remote access should consider two-factor authentication.
c. The Risk Assessment and SSP shall document any remote access of PII, and the remote access shall be approved by the DAA prior to implementation.
d. 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. Any two-factor authentication shall be based on agency-controlled certificates or hardware tokens issued directly to each authorized user.
e. 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 SSP.

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.

DHS Policy
a. Components shall provide continuous monitoring of their networks for security events or outsource this requirement to the DHS SOC.
b. Components shall report any event that is a security incident to the DHS SOC.

5.4.3 Network Connectivity

DHS Policy
a. Components shall ensure that appropriate identification and authentication controls, audit logging, and access controls are implemented on every network component.
b. Interconnections between DHS and non-DHS IT 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 interconnect service agreements.
c. Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA). Interconnections between DHS Components shall require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. ISAs shall be signed by both DAAs or by the official designated by the DAA to have

DHS Policy
signatory authority.
d. ISAs shall be reissued every three years or whenever any significant changes have been made to any of the interconnected systems.
e. ISAs shall be reviewed as a part of the annual FISMA self-assessment.

5.4.4 Firewalls

DHS Policy
a. Components shall restrict physical access to firewalls to authorized personnel.
b. Components shall implement strong identification and authentication for administration of the firewalls.
c. Components shall encrypt remote maintenance paths to the firewalls.
d. Components shall conduct quarterly testing to ensure that firewall configurations are correct.
e. Component SOCs shall ensure reports on security operations status and incident reporting are provided to the CISO Security Operations Program Director as required.

5.4.5 Internet Security

DHS Policy
a. Any direct connection of DHS networks to the Internet or to extranets must occur through firewalls that have been certified and accredited.
b. Firewalls shall be configured to prohibit any protocol or service that is not explicitly permitted.
c. Components shall ensure that all executable code, including mobile code (e.g., ActiveX, JavaScript), is reviewed and approved by an appropriate senior official prior to the code being allowed to execute within the 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 IT systems.”]
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, etc.) and is approved by the Component shall be used instead.
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, etc.) and is approved by the Component shall be used instead.

5.4.6 Email Security

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

A relationship has been established between the email Steward and the DHS SOC to enable communications. DHS SOC personnel will be trained to respond to incidents pertaining to email security and will assist the email Steward as necessary.

DHS Policy
Components shall provide appropriate security for their email systems and email clients by:
a. Correctly securing, installing, and configuring the underlying operating system.
b. Correctly securing, installing, and configuring mail server software.
c. Securing and filtering email content.
d. Deploying appropriate network protection mechanisms, such as: <ul style="list-style-type: none"> – Firewalls – Routers – Switches – Intrusion detection systems.
e. Securing mail clients.
f. Conducting mail server administration in a secure manner. This includes: <ul style="list-style-type: none"> – Performing regular backups – Performing periodic security testing – Updating and patching software – Reviewing audit logs at least weekly.

5.4.7 Personal Email Accounts

DHS Policy
DHS employees or contractors shall not transmit FOUO information to any personal email account.

5.4.8 Testing and Vulnerability Management

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

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

advisories, and system security testing such as automated vulnerability scanning or security tests and evaluations (ST&E).

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

DHS Policy
<p>a. Components shall conduct vulnerability assessments and/or testing to identify security vulnerabilities on IT systems containing sensitive information annually or whenever significant changes are made to the IT systems. This should include scanning for unauthorized wireless devices. Evidence that annual assessments have been conducted should be included with Security Assessment Reports (SAR).</p>
<p>b. 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 SDLC support.</p>
<p>c. Anyone within DHS may request to be added to the ISVM distribution list. Those wishing to be added must provide a DHS email address and obtain management approval. ISVMs contain sensitive, "For Official Use Only," information and must not be forwarded to non-DHS email accounts.</p> <p>Although ISVM messages can be sent to anyone, <i>only Component ISSMs</i> or their designated representatives may acknowledge receipt of messages, report compliance with requirements or notify the granting of waivers.</p>
<p>d. Components should report compliance with the ISVM message within the specified timeframe. Components unable to meet the designated compliance timeframe must submit documentation of a waiver request via the DHS SOC Online Portal (https://soconline.dhs.gov)</p>
<p>e. ISSMs shall ensure coordination among the DHS SOC, the Component SOC, and the Information Security Vulnerability Management (ISVM) Program when vulnerability assessment responsibilities encompass more than one Component.</p>

5.4.9 Peer-to-Peer Technology

DHS Policy
<p>Peer-to-peer software is not authorized on DHS computers or on any computer or IT system that might be connected to the DHS network.</p>

5.5 Cryptography

Cryptography is a branch of mathematics that is based on the transformation of data. Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and the transformation of ciphertext into plaintext by decryption. Cryptography relies on two basic components: an algorithm (e.g., Advanced Encryption Standard [AES]) and a key. The algorithm is the mathematical function used for encryption or decryption, and the key is the parameter used in the transformation.

There are two basic types of cryptography: secret key systems (also call symmetric systems) and public key systems (also called asymmetric systems). In secret key systems, the same key is used for both encryption and decryption; that is, all parties participating in the communication share a single key. In public key systems, there are two keys: a public key and a private key. The public key used for encryption is different from the private key used for decryption. The two keys are mathematically related, but the private key cannot be determined from the public key.

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

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

5.5.1 Encryption

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

DHS Policy
<p>a. Components shall identify IT systems transmitting sensitive information that may require protection based on a risk assessment. If encryption is required, the following methods are acceptable for encrypting sensitive information:</p> <ul style="list-style-type: none"> – Products using Advanced Encryption Standard (AES) algorithms that have been validated under FIPS 140-2. (Note: The use of triple DES [3DES] and FIPS 140-1 is no longer permitted. A waiver is required for systems where AES cannot currently be used.) – NSA Type 2 or Type 1 encryption.
<p>b. Components shall develop and maintain encryption plans for their sensitive IT systems.</p>
<p>c. Components shall use only cryptographic modules that have been validated in accordance with FIPS 140-2.</p>

5.5.2 Public Key Infrastructure

A public key infrastructure (PKI) is an architecture that provides the means to bind public keys to their owners' private keys and helps in the distribution of reliable credentials in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates, which contain information such as the owner's name and the associated public key, are issued by a reliable certification authority (CA). Reliable identification of individuals is an inherently governmental activity. In order to establish and maintain the trust required to support DHS missions, the root certificate must be controlled by the DHS.

Any DHS Component that implements a PKI or CA for a PKI must ensure that its CA is subordinate to the DHS Root CA. The use of self-signed certificates has minimal security value and violates Executive Office Directives. The use of any non-DHS service provider for CA or PKI support is inconsistent with DHS Mission requirements and must be approved by the CISO.

DHS Policy
a. PKI policy oversight shall be provided at the Department level by a PKI Policy Authority (PKI PA). The CISO shall be the PKI PA.
b. PKI operational oversight shall be provided at the Department level by a PKI Operational Authority (PKI OA) appointed by the PKI PA.
c. The DHS PKI shall be governed by a DHS X.509 Certificate Policy (DHS CP). The DHS CP shall be approved by the PKI PA.
d. The DHS CP must comply with the U.S. Federal PKI Certificate Policy for the Federal Bridge CA, at the high, medium, and basic assurance levels.
e. DHS shall have a single High Assurance Root CA. All additional CAs within DHS must be subordinate to the DHS Root CA. The requirements and process for becoming a subordinate CA to the DHS Root CA shall be specified in the DHS CP.
f. The DHS Root CA shall cross-certify with the Federal Bridge CA at the high, medium, and basic assurance levels.
g. Every DHS CA shall operate under an X.509 Certificate Practices Statement (CPS). The CPS for each CA must comply with the DHS CP. The DHS PKI PA must approve each CPS.
h. All DHS CAs shall undergo a compliance audit on a regular basis as required by CP. The DHS PKI PA shall specify a DHS PKI Auditor to review compliance audits.
i. All operational PKI facilities should be established in accordance with the requirements commensurate with the CA's assurance level as well as its intended use. Location/protection of the authority will be determined by its level of assurance. Measures to ensure continuity of operations of the certificate authority should be taken that are at least equal to the measures of the system being supported.
j. A DHS PKI archive facility shall be established to store PKI records, as required by the CP and CPSs.
k. Certificates that are issued by test, pilot, third party, or other CAs in DHS and that are not established as a subordinate CA to the DHS Root CA shall not be used to protect sensitive DHS data, or to authenticate to DHS operational systems containing sensitive data.

5.5.3 Public Key/Private Key

The recipient of public key certificates is referred to as a subscriber. A subscriber can be a human (e.g., an employee or contractor), an organization, an application, a code signer (e.g., digitally signs released software to enable users to authenticate its source, legitimacy, and integrity), or a device (e.g., a web server or VPN server.) Registrars are trusted PKI officials

who administer the process that results in a CA issuing or revoking public key certificates for each subscriber. As part of the PKI registration process, a public key/private key pair is generated in a hardware or software cryptographic module that is under the control of the subscriber. The private key remains under the sole possession of the subscriber. A CA enters the public key into an electronic public key certificate that also identifies the owner of the key, i.e. the subscriber. The trusted CA digitally signs the certificate thereby binding the public key to the subscriber, and makes the signed certificate available for use by other subscribers.

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

DHS Policy
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.
b. Separate public/private key pairs must be used for encryption and digital signature by device subscribers whenever supported by the protocols native to the type of device.
c. A human sponsor shall represent each organization, application, code-signing, and device subscriber when it applies for one or more certificates from a DHS CA.
d. A mechanism shall be provided for each DHS CA to enable PKI registrars to determine the eligibility of each proposed human, organization, application, code signer, or device to receive one or more certificates.
e. A mechanism shall be provided for each DHS CA to enable PKI registrars to determine the authorized human sponsor for each organization, application, code signer, or device.
f. Human subscribers shall be responsible for the security of and use of their private keys. 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.
g. The sponsor of an organization, application, code-signing, or device subscriber shall be responsible for the security of and use of the subscriber's private keys.
h. Ensure that only private keys that correspond to a public key on a certificate issued to an organization or code-signing subscriber are authorized to be used by more than one person. If more than one person is authorized to use the key, ensure that auditable records are kept to maintain individual accountability for each use of the private key.
i. Every human subscriber shall read, understand, and sign a DHS PKI Subscriber Agreement for Human Users as a pre-condition for receiving certificates from a DHS CA.
j. Every sponsor shall read, understand, and sign a DHS PKI Subscriber Agreement for Sponsors as a

DHS Policy

pre-condition for receiving certificates from a DHS CA for the nonhuman subscriber they sponsor.
--

5.6 Virus Protection

DHS Policy

a. ISSMs shall establish and enforce Component-level virus protection control policies.
--

b. Components shall implement a defense-in-depth strategy that:
--

- | |
|---|
| <ul style="list-style-type: none"> – Installs antivirus software on desktops and servers – 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. |
|---|

c. Components may implement appropriate file/protocol/content filtering to protect their data and networks in accordance with their Internet usage policy.

5.7 Product Assurance

DHS Policy

a. Information Assurance (IA) shall be considered a requirement for all systems used to enter, process, store, display, or transmit sensitive or national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated commercial off-the-shelf (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.
--

b. <i>Strong preference</i> 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:

- | |
|---|
| <ul style="list-style-type: none"> – The NIST FIPS validation program. – The National Security Agency (NSA)/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program – The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement |
|---|

c. The evaluation and validation of COTS IA and IA-enabled IT products shall be conducted by accredited commercial laboratories or by NIST.
--

6.0 DOCUMENT CHANGE REQUESTS

Changes to this DHS Sensitive Systems Policy Directive 4300A and to the DHS 4300A Sensitive Systems Handbook can be requested by filling out the form included as Attachment P to the handbook.

7.0 QUESTIONS AND COMMENTS

For clarification of DHS IT security policies or procedures, contact the DHS Director for IT Security Policy at INFOSEC@dhs.gov.