



**Homeland
Security**

DHS 4300A
Sensitive Systems Handbook

Version 9.1
July 24, 2012

Protecting the Information that Secures the Homeland

This page intentionally left blank

Contents

1.0	INTRODUCTION.....	1
1.1	Information Security Program and Implementation Guidelines	1
1.2	Authorities.....	2
1.3	Policy Overview.....	2
1.4	Definitions.....	3
1.4.1	Sensitive Information.....	3
1.4.2	Public Information	3
1.4.3	National Security Information.....	3
1.4.4	Classified National Security Information.....	3
1.4.5	National Intelligence Information	3
1.4.6	Foreign Intelligence Information	4
1.4.7	Information Technology.....	4
1.4.8	DHS System.....	4
1.4.9	Component.....	5
1.4.10	Trust Zone.....	5
1.4.11	Continuity of Operations.....	5
1.4.12	Continuity of Operations Plan.....	5
1.4.13	Essential Functions	6
1.4.14	Vital Records	6
1.4.15	Federal Information Security Management Act.....	6
1.4.16	Personally Identifiable Information	8
1.4.17	Sensitive Personally Identifiable Information.....	8
1.4.18	Privacy Sensitive System	8
1.4.19	Strong Authentication	8
1.4.20	Two-Factor Authentication.....	8
1.5	Waivers and Exceptions.....	8
1.5.1	Waivers	8
1.5.2	Exceptions.....	9
1.5.3	Waiver or Exception Requests.....	9
1.5.4	Requests for Exception to U.S. Citizenship Requirement	11
1.6	Electronic Signature.....	11
1.7	Information Sharing	12
1.8	Threats.....	13
1.8.1	Internal Threats	13
1.8.2	Criminal Threats	13
1.8.3	Foreign Threats	14
1.8.4	Lost or Stolen Equipment	14
1.8.5	Supply Chain Threats.....	14
1.9	Changes to Policy.....	14
2.0	ROLES AND RESPONSIBILITIES.....	16

2.1	Information Security Program Roles	16
2.1.1	DHS Senior Agency Information Security Officer	16
2.1.2	DHS Chief Information Security Officer	16
2.1.3	Component Chief Information Security Officer	18
2.1.4	Component Information Systems Security Manager	21
2.1.5	Risk Executive	22
2.1.6	Authorizing Official	23
2.1.7	Security Control Assessor	23
2.1.8	Information Systems Security Officer	24
2.2	Other Roles	25
2.2.1	Secretary of Homeland Security	25
2.2.2	Under Secretaries and Heads of DHS Components	26
2.2.3	DHS Chief Information Officer	27
2.2.4	Component Chief Information Officer	28
2.2.5	DHS Chief Security Officer	29
2.2.6	DHS Chief Privacy Officer	29
2.2.7	DHS Chief Financial Officer	30
2.2.8	Program Managers	31
2.2.9	System Owners	31
2.2.10	Common Control Provider	32
2.2.11	DHS Employees, Contractors, and Others Working on Behalf of DHS	32
3.0	MANAGEMENT POLICIES	33
3.1	Basic Requirements	33
3.2	Capital Planning and Investment Control	34
3.2.1	Capital Planning and Investment Control Process	36
3.3	Contractors and Outsourced Operations	37
3.4	Performance Measures and Metrics	39
3.5	Continuity Planning for Critical DHS Assets	40
3.5.1	Continuity of Operations Planning	41
3.5.2	Contingency Planning	44
3.6	System Engineering Life Cycle	48
3.6.1	Planning	50
3.6.2	Requirements Definition	50
3.6.3	Design	51
3.6.4	Development	51
3.6.5	Test	51
3.6.6	Implementation	52
3.6.7	Operations and Maintenance	52
3.6.8	Disposition	52
3.7	Configuration Management	52
3.8	Risk Management	56
3.8.1	Risk Assessment	57
3.8.2	Risk Mitigation	58
3.8.3	Evaluation and Assessment	58
3.9	Security Authorization and Security Assessments	58

3.9.1	FIPS 199 Categorization and the NIST SP 800-53 Controls	64
3.9.2	Privacy Impact Assessment.....	65
3.9.3	E-Authentication.....	65
3.9.4	Risk Assessment	65
3.9.5	Security Plan	66
3.9.6	Contingency Plan	66
3.9.7	Security Control Assessment Plan	67
3.9.8	Contingency Plan Testing	67
3.9.9	Security Assessment Report.....	69
3.9.10	Plan of Action and Milestones	69
3.9.11	Authorization to Operate Letter	69
3.9.12	Annual Self-Assessments.....	70
3.10	Information Security Review and Assistance	71
3.10.1	Review and Assistance Management and Oversight	72
3.10.2	Information Security Assistance	72
3.10.3	Information Security Reviews.....	73
3.11	Security Working Groups and Forums	73
3.11.1	CISO Council.....	73
3.11.2	DHS Information Security Training Working Group	73
3.11.3	DHS Security Policy Working Group.....	74
3.12	Information Security Policy Violation and Disciplinary Action.....	74
3.13	Required Reporting.....	75
3.14	Privacy and Data Security	76
3.14.1	Personally Identifiable Information	76
3.14.2	Privacy Threshold Analyses.....	78
3.14.3	Privacy Impact Assessments	79
3.14.4	System of Record Notices.....	80
3.14.5	Protecting Privacy Sensitive Systems	80
3.14.6	Privacy Incident Reporting	82
3.14.7	E-Authentication	83
3.15	DHS CFO Designated Systems.....	84
3.16	Social Media	87
3.17	Health Insurance Portability and Accountability Act.....	88
3.18	Cloud Services	89
4.0	OPERATIONAL CONTROLS	91
4.1	Personnel.....	91
4.1.1	Personnel Screening and Position Categorization	91
4.1.2	Rules of Behavior	94
4.1.3	Access to Sensitive Information	96
4.1.4	Separation of Duties.....	96
4.1.5	Information Security Awareness, Training, and Education	98
4.1.6	Separation from Duty.....	102
4.2	Physical Security.....	104
4.2.1	General Physical Access	104
4.2.2	Sensitive Facility.....	108

4.3	Media Controls.....	109
4.3.1	Media Protection.....	109
4.3.2	Media Marking and Transport	111
4.3.3	Media Sanitization and Disposal	113
4.3.4	Production, Input/Output Controls.....	116
4.4	Voice Communications Security	117
4.4.1	Private Branch Exchange	117
4.4.2	Telephone Communications	122
4.4.3	Voice Mail	123
4.5	Data Communications.....	124
4.5.1	Telecommunications Protection Techniques	124
4.5.2	Facsimiles	126
4.5.3	Video Teleconferencing.....	127
4.5.4	Voice Over Data Networks.....	129
4.6	Wireless Network Communications	131
4.6.1	Wireless Systems	133
4.6.2	Wireless Portable Electronic Devices.....	135
4.6.3	Wireless Tactical Systems	141
4.6.4	Radio Frequency Identification.....	144
4.7	Overseas Communications.....	145
4.8	Equipment.....	146
4.8.1	Workstations	147
4.8.2	Laptop Computers and Other Mobile Computing Devices	148
4.8.3	Personally Owned Equipment and Software.....	150
4.8.4	Hardware and Software.....	151
4.8.5	Personal Use of Government Office Equipment and DHS Systems/Computers.....	153
4.8.6	Wireless Settings for Peripheral Equipment.....	157
4.9	Department Information Security Operations.....	157
4.9.1	Security Incidents and Incident Response and Reporting.....	160
4.9.2	Law Enforcement Incident Response.....	165
4.9.3	Definitions and Incident Categories.....	166
4.10	Documentation.....	167
4.11	Information and Data Backup.....	169
4.12	Converging Technologies	172
5.0	TECHNICAL CONTROLS.....	175
5.1	Identification and Authentication.....	175
5.1.1	Passwords.....	177
5.2	Access Control.....	180
5.2.1	Automatic Account Lockout.....	183
5.2.2	Automatic Session Termination.....	184
5.2.3	Warning Banner	185
5.3	Auditing	186
5.4	Network and Communications Security	189
5.4.1	Remote Access and Dial-In.....	189

5.4.2	Network Security Monitoring	190
5.4.3	Network Connectivity	193
5.4.4	Firewalls and Policy Enforcement Points	198
5.4.5	Internet Security	200
5.4.6	Email Security	204
5.4.7	Personal Email Accounts	208
5.4.8	Testing and Vulnerability Management	209
5.4.9	Peer-to-Peer Technology	213
5.5	Cryptography	214
5.5.1	Encryption	215
5.5.2	Public Key Infrastructure	216
5.5.3	Public Key/Private Key	225
5.6	Malware Protection	229
5.6.1	Types of Malware	229
5.6.2	How Malware Affects Systems	229
5.6.3	Procedures When Malware Is Detected On a System	230
5.7	Product Assurance	232
5.8	Supply Chain	233
6.0	DOCUMENT CHANGE REQUESTS	237
7.0	QUESTIONS AND COMMENTS	237
APPENDIX A	ACRONYMS AND ABBREVIATIONS	238
APPENDIX B	GLOSSARY	246
APPENDIX C	REFERENCES	251
APPENDIX D	DOCUMENT CHANGE HISTORY	255

Enclosure 1—DHS Secure Baseline Configuration Guides

- Cisco Router Secure Baseline Configuration Guide
- HP-UX Secure Baseline Configuration Guide
- Linux Secure Baseline Configuration Guide
- Solaris Secure Baseline Configuration Guide
- Solaris 10 Secure Baseline Configuration Guide
- Windows Secure Baseline Configuration Guide
- SQL Server Secure Baseline Configuration Guide
- ORACLE Secure Baseline Configuration Guide
- Legacy Windows NT Configuration Guidance
- Guidance for Securing Windows NT

- Level One Benchmark Windows NT 4-0 Operating Systems V1.0.5
- Guide to Securing Microsoft Windows NT Network
- Addendum to the NSA Guide to Securing Microsoft Windows NT Networks and NSA Guides to Securing Windows 2000

- Windows 2003 Server/Windows XP/Windows Vista Secure Baseline Configuration Guide

Attachment A—Requirements Traceability Matrix [removed as of v9.1]

Attachment B—Waivers and Exceptions Request Form

Attachment C—Information Systems Security Officer Designation Letter

Attachment D—Type Authorization

Attachment E—FISMA Reporting

Attachment F—Incident Response and Reporting

Attachment G—Rules of Behavior

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

Attachment I—Workstation Logon, Logoff, and Locking Procedures [removed as of v9.1]

Attachment J—Requesting Exceptions to Citizenship Requirement

Attachment K—IT Contingency Plan Template

Attachment L—Password Management

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

Attachment N—Preparation of Interconnection Security Agreements

Attachment O—Vulnerability Assessment Program

Attachment P—Document Change Requests

Attachment Q1—Wireless Systems

Attachment Q2—Wireless Portable Electronic Devices

Attachment Q3—Wireless Tactical Systems

Attachment Q4—Sensitive RFID Systems

Attachment R—Compliance Framework for CFO Designated Financial Systems

Attachment S—Compliance Framework for Privacy Systems

Attachment S1—Managing CREs Containing SPII

Attachment T—Aeronyms and Abbreviations [removed as of v9.1]

Attachment X—Social Media

This page intentionally left blank

1.0 INTRODUCTION

This handbook is a compilation of the best practices used by Department of Homeland Security (DHS) Components and includes requirements contained in various National Institute of Standards and Technology (NIST) publications, Office of Management and Budget (OMB) direction, and Congressional and Executive mandates.

The Handbook serves as a foundation on which Components can develop, build, and implement information security programs; it provides specific techniques and procedures for implementing the requirements of the DHS Information Security Program for Sensitive Systems. These baseline security requirements (BLSR) are generated by the DHS information security policies published in “DHS Sensitive Systems Policy Directive 4300A.” BLSRs must be addressed when developing and maintaining information security documents.

The scope and contents of this handbook will be updated as new capabilities are added to DHS systems, as security standards are upgraded, and as a result of user experience and comment.

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

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

1.1 Information Security Program and Implementation Guidelines

The DHS Information Security Program provides a baseline of policies, standards, and guidelines for DHS Components. This Handbook 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 DHS information system infrastructure and operations. Policy elements are designed to be broad in scope. Implementation information can often be found in specific NIST publications, such as NIST Special Publication (SP) 800-53, “Recommended Security Controls for Federal Systems and Organizations.”

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

Policy elements are effective when issued. Any policy elements that have not been implemented within ninety (90) days shall be considered a weakness and either a system or program Plan of Action and Milestones (POA&M) must be generated by the Component for the identified weaknesses. When this Policy Directive is changed, the CISO will ensure that appropriate

changes in DHS Security Compliance tools, Risk Management System (RMS), and Trusted Agent FISMA¹ (TAF); tool changes are made available to the Department within forty-five (45) days of the changes.

1.2 Authorities

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

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

- E-Government Act of 2002, including Title III, Federal Information Security Management Act (FISMA), Public Law 107-347, codified at 44 USC. §§ 3541-3549
- OMB Circular A-130, “Management of Federal Information Resources,” revised, November 30, 2000
- DHS Management Directive (MD) 140-01, “Information Technology Systems Security,” July 31, 2007
- DHS Sensitive Systems Policy Directive 4300A
- NIST Federal Information Processing Standard (FIPS) 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006”
- NIST SP 800-53, Rev 3, “Recommended Security Controls for Federal Information Systems and Organizations,” August 2009, with updated errata May 01, 2010”

1.3 Policy Overview

DHS information security policies define the security management structure and foundation needed to measure progress and compliance. Policies in this document are organized in three sections:

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

¹ FISMA: *Federal Information Security Management Act, 44 U.S.C 3541*

1.4 Definitions

The definitions in this section apply to the policies and procedures discussed in this document. Other definitions may be found in the [“National Information Assurance \(IA\) Glossary,”](#) and in [“Privacy Incident Handling Guidance and the Privacy Compliance.”](#)

1.4.1 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 numbers; trade secrets; system vulnerability information; pre-solicitation procurement documents, such as statements of work; and information pertaining to law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies in internal controls are also sensitive information because of the potential damage that could be caused by the misuse of this information. System vulnerability information about a financial system shall be considered Sensitive Financial Information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access.

1.4.2 Public Information

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

1.4.3 National Security Information

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

1.4.4 Classified National Security Information

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

1.4.5 National Intelligence Information

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

“The terms ‘national intelligence’ and ‘intelligence related to national security’ refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that – “(A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and “(B) that involves – (i) threats to the

United States, its people, property, or interests; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on United States national or homeland security.”

1.4.6 Foreign Intelligence Information

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

1.4.7 Information Technology

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

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

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

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

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

1.4.8 DHS System

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

1.4.8.1 General Support System

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

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

1.4.8.2 Major Application

A *major application* (MA) is an automated information system (AIS) that “requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.”² [Note: All Federal applications require some level of protection.] Certain applications, because of the information they contain, however, require special management oversight and should be treated as MAs. An MA is distinguishable from a GSS by the fact that it is a discrete application, whereas a GSS may support multiple applications. Each MA must be under the direct oversight of a Component CISO or Information System Security Manager (ISSM), and must have an ISSO assigned.

1.4.9 Component

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

1.4.10 Trust Zone

A *Trust Zone* consists of any combination of people, information resources, data systems, and networks that are subject to a shared security policy (a set of rules governing access to data and services). For example, a Trust Zone may be set up between different network segments that require specific usage policies based on information processed, such as law enforcement information.

1.4.11 Continuity of Operations

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

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

1.4.12 Continuity of Operations Plan

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

² OMB Circular A-130

1.4.13 Essential Functions

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

1.4.14 Vital Records

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

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

1.4.15 Federal Information Security Management Act

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

- (1) Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.
- (2) Policies and procedures that:
 - a. Are based on the risk assessments required by paragraph (1) above
 - b. Cost-effectively reduce information security risks to an acceptable level
 - c. Ensure that information security is addressed throughout the life cycle of each agency information system
 - d. Ensure compliance with
 - i. Other applicable Federal policies and procedures as may be prescribed by OMB and NIST Minimally acceptable system configuration requirements, as determined by the agency
 - ii. Any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President

- (3) Subordinate plans for providing adequate information security for networks, facilities, and information systems, as appropriate;
- (4) Security awareness training to inform personnel, including contractors, others working on behalf of DHS, and others who use information systems supporting operations and assets of the Department. Such training shall convey knowledge of
 - a. Information security risks associated with their activities
 - b. Their responsibility to comply with agency policies and procedures designed to reduce these risks
- (5) Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually. This testing:
 - a. Shall include testing of management, operational, and technical controls of every information system identified in the Department's inventory
 - b. May include testing relied on by the Office of Inspector General (OIG)
- (6) A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the Department's information security policies, procedures, and practices
- (7) Procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines published by the United States Computer Emergency Readiness Team (US-CERT)
 - a. Mitigating risks associated with incidents before substantial damage is done
 - b. Notifying and consulting with US-CERT
 - c. Notifying and consulting with:
 - i. Law enforcement agencies and relevant OIG
 - ii. An office designated by the President for any incident involving a national security system
 - iii. Other agency or offices, as required
- (8) Plans and procedures to ensure continuity of operations (CO) for information systems that support the operations and assets of the Department

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

- Developing and maintaining information security policies, procedures, and control techniques that address all applicable requirements
- Training and overseeing personnel with significant information security responsibilities
- Assisting senior Department officials with respect to their responsibilities under the statute

- Ensuring that the Department has sufficient trained personnel to ensure the Department's compliance with the statute and related policies, procedures, standards, and guidelines
- Ensuring that the Department CIO, in coordination with other senior Department officials, reports annually to the Secretary on the effectiveness of the Department's information security program, including the progress of remedial actions

1.4.16 Personally Identifiable Information

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

1.4.17 Sensitive Personally Identifiable Information

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

1.4.18 Privacy Sensitive System

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

1.4.19 Strong Authentication

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

1.4.20 Two-Factor Authentication

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

1.5 Waivers and Exceptions

1.5.1 Waivers

Components may request waivers to, or exceptions from, any portion of this Policy Directive for up to six (6) months at any time they are unable to fully comply with a Policy Directive requirement. Waiver requests are routed through the Component's ISSO for the system, to the Component's CISO or ISSM, and then to the DHS CISO. All submitters shall coordinate with the Authorizing Official (AO) prior to submission. If a material weakness is reported in an audit report, and the weakness is not scheduled for remediation within twelve (12) months, the Component must submit a waiver request to the DHS CISO. If the material weakness is in a

financial system, the Component Chief Financial Officer (CFO) must also approve the waiver request before sending to the DHS CISO.

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

1.5.2 Exceptions

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

The risk that results from the exception also must be approved and accepted by the AO and by the Component CFO if the system is a financial or mixed financial system.

1.5.3 Waiver or Exception Requests

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

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

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

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

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

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

Policy ID	DHS Policy Statements	Relevant Controls
1.5.3.a	This Policy Directive and the DHS 4300A Sensitive Systems Handbook apply to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS data unless an approved waiver or	---

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

1.5.4 Requests for Exception to U.S. Citizenship Requirement

Special procedures apply for exception to the requirement that persons accessing DHS systems be U.S. citizens. Under normal circumstances, only U.S. citizens are allowed access to DHS systems and networks; but there is a need at times to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to pertinent policies are treated separately from standard exceptions and waivers. The approval chain for an exception to the U.S. citizenship requirement flows through the Component Head, the Office of Security, and the CIO. An electronic form for requesting exceptions to the U.S. citizenship requirement is published in this Handbook's Attachment J, "Requesting Exceptions to Citizenship Requirement."

Policy ID	DHS Policy Statements	Relevant Controls
1.5.4.a	Persons of dual citizenship, where one of the citizenships includes U.S. citizenship, shall be treated as U.S. citizens for the purposes of this Policy Directive.	---
1.5.4.b	The System Owner shall submit each request for exception to the U.S. Citizenship policy to the Component Head. The Component Head shall obtain concurrence from the DHS Chief Security Officer (CSO) and CIO prior to the approval becoming effective.	PS-3
1.5.4.c	Additional compensating controls shall be maintained for foreign nationals, based on nations lists maintained by the DHS CSO.	PS-3

1.6 Electronic Signature

Pursuant to Sections 1703 and 1705 of the Government Paperwork Elimination Act (GPEA), OMB Memorandum M-00-10, "Procedures and Guidance on Implementing of the Government Paperwork Elimination Act,"³ requires executive agencies to provide the option for electronic maintenance, submission, and disclosure of information when practicable as a substitute for paper, and to use and accept electronic signatures.

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

Electronic signature solutions must be approved by the Component CISO.

³ *Government Paperwork Elimination Act (GPEA), Pub L 105-277, 44 USC 3501 (note) provide for the use*

Policy ID	DHS Policy Statements	Relevant Controls
1.6.a	For DHS purposes, electronic signatures are preferred to pen and ink or facsimile signatures in all cases, except where pen and ink signatures are required by public law, statute, Executive Order, or other agency requirement.	---
1.6.b	Wherever practicable, Components shall use and accept electronic signatures.	---
1.6.c	Components shall accept electronic signatures whenever the signature's digital certificate is current, electronically verifiable, and issued by a medium or high assurance DHS Certification Authority (CA) or other medium or high CA under the Federal Bridge Certification Authority (FBCA) or Common Authority.	---
1.6.d	Components shall accept and be able to verify Personal Identity Verification (PIV) credentials issued by other Federal agencies as proof of identity.	---
1.6.e	As mandated by the Government Paperwork Elimination Act (GPEA) and OMB M-00-10, Components shall provide for the use and acceptance of electronic signatures when practicable.	---

1.7 Information Sharing

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

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

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

- Entering incident information into the DHS SOC incident database

- Generating preformatted incident reports

- Initiating queries of the incident database

- Viewing FISMA incident reporting numbers

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

Automating portions of the vulnerability assessment program

1.8 Threats

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

Information systems are often connected to different parts of an organization; interconnected with other organizations' systems; and with the Internet. Remote access for telecommuting and building management services (e.g., badge systems; heating, ventilating, and air-conditioning (HVAC); and entry) may require additional connections, all of which introduce additional risks.

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

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

1.8.1 Internal Threats

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

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

1.8.2 Criminal Threats

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

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

1.8.3 Foreign Threats

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

Wireless communications are easily eavesdropped on using commercially available equipment, and it is relatively easy to detect and exploit wireless access points. Employees overseas should assume their wireless communications (BlackBerry, cell phone, etc) are being monitored.

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

1.8.4 Lost or Stolen Equipment

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

1.8.5 Supply Chain Threats

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

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

1.9 Changes to Policy

Procedures and guidance for implementing this policy are outlined in a companion publication, *DHS 4300A Sensitive Systems Handbook* and its attachments. The Handbook serves as a foundation for Components to use in developing and implementing their information security programs.

For interpretation or clarification of DHS information security policies found in this policy document and of the procedures and guidance found in the *DHS 4300A Sensitive Systems Handbook*, contact the DHS CISO at infosec@dhs.gov.

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

Policy ID	DHS Policy Statements	Relevant Controls
1.9.a	The DHS CISO shall be the authority for interpretation, clarification, and	PL-1

Policy ID	DHS Policy Statements	Relevant Controls
	modification of the <i>DHS Sensitive Systems Policy Directive 4300A</i> and for the <i>DHS 4300A Sensitive Systems Handbook</i> (inclusive of all appendices and attachments).	
1.9.b	The DHS CISO shall update the <i>DHS Sensitive Systems Policy Directive 4300A</i> and the <i>DHS 4300A Sensitive Systems Handbook</i> at least annually.	PL-1

2.0 ROLES AND RESPONSIBILITIES

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

2.1 Information Security Program Roles

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

2.1.1 DHS Senior Agency Information Security Officer

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

2.1.2 DHS Chief Information Security Officer

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

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

Policy ID	DHS Policy Statements	Relevant Controls
2.1.2.a	The DHS CISO shall implement and manage the DHS-wide Information Security Program.	PL-1, PM-2
2.1.2.b	The DHS CISO will serve as the CIO's primary liaison with the organization's Authorizing Officials (AO), information system owners and Information Systems Security Officers (ISSO).	---

The DHS CISO:

Implements and manages the Department-wide Information Security Program and ensures compliance with the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) directives, and other Federal requirements

- Issues Department-wide information security policy, guidance, and architecture requirements for all DHS systems and networks. These policies shall incorporate National Institute of

Standards and Technology (NIST) guidance, as well as all applicable OMB memorandums and circulars

- Facilitates development of subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems
- Serves as the principal Departmental liaison with organizations outside DHS in matters relating to information security
- Reviews and approves the tools, techniques, and methodologies planned for use in certifying and authorizing DHS systems, and for reporting and managing systems-level FISMA data. This responsibility includes reviews and approval of Security Control Assessment plans, Contingency Plans, and security risk assessments.
- Consults with the DHS Chief Security Officer (CSO) on matters pertaining to physical security, personnel security, information security, investigations, and Sensitive Compartmented Information (SCI) systems, as they relate to information security and infrastructure
- Develops and implements procedures for detecting, reporting, and responding to information security incidents
- Ensures preparation and maintenance of plans and procedures to provide continuity of operations (CO) for information systems
- Ensures that Department personnel, contractors, and others working on behalf of DHS receive information security awareness training
- Chairs the CISO Council. The Council is composed of all Component CISOs, and is the Department's sole coordination body for any issues associated with information security policy, management, and operations. Component Information Systems Security Managers (ISSM) will be invited to CISO Council meetings as required
- Maintains a comprehensive inventory of all general support systems (GSS) and major applications (MA) in use within the Department
 - Security management for every GSS shall be under the direct oversight of either the DHS CISO (for enterprise systems) or a Component CISO/ISSM (for Component-specific GSSs)
 - MAs must be under the direct control of either a Component CISO or Component ISSM
- Maintains a repository for all Information Assurance (IA) security authorization process documentation and modifications
- Performs security reviews for all planned information systems acquisitions over \$2.5 million and for additional selected cases
- Provides oversight of all security operations functions within the Department
- Maintains classified threat assessment capability in support of security operations
- Performs annual program assessments for each of the Components

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

2.1.3 Component Chief Information Security Officer

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

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

The following Components shall have a fulltime CISO:

- Customs and Border Protection (CBP)
- Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- United States Secret Service (USSS)
- United States Coast Guard (USCG)
- Federal Emergency Management Agency (FEMA)
- United States Citizenship and Immigration Services (USCIS)

- Federal Law Enforcement Training Center (FLETC)
- Headquarters, Department of Homeland Security
- Office of Intelligence and Analysis (I&A)
- National Protection and Programs Directorate (NPPD)
- Science and Technology (S&T)

Component CISOs shall:

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

- Ensure execution of the DHS Logging Strategy detailed in this Handbook
- Ensure adherence to the DHS Secure Baseline Configuration Guides (Enclosure 1 to this Handbook)
- Ensure reporting of vulnerability scanning activities to the DHS SOC, in accordance with *DHS 4300A Sensitive Systems Handbook* Attachment O, “Vulnerability Management Program.”
- Develop and maintain a Component-wide information security program in accordance with Department policies and guidance
- Implement Department information security policies, procedures, and control techniques to ensure that all applicable requirements are met
- Update Security Training section within DHS FISMA Manager resource at least once per quarter
- Ensure training and oversight of personnel with significant responsibilities for information security
- Oversee the Component’s Security Authorization process for GSSs and MAs
- Maintain an independent Component-wide assessment program to ensure that there is a consistent approach to controls effectiveness testing
- Ensure that an appropriate SOC performs an independent network assessment as part of the assessment process for each authorized application
- Ensure that enterprise security tools are utilized
- Oversee all Component security operations functions, including the Component SOCs
- Ensure that external providers who operate information systems on behalf of the Component meet the same security requirements as required for information and information systems.
- Ensure an acceptable level of trust in the external service; or using compensating controls to secure information or the process flow, accepting a greater degree of risk, or reducing the functionality to the extent necessary to make the risk acceptable

Component CISO qualifications include:

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

- Ability to serve as the Component Risk Executive

2.1.4 Component Information Systems Security Manager

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

Policy ID	DHS Policy Statements	Relevant Controls
2.1.4.a	Component ISSMs shall serve as the principal interface between the HQ CISO, Component ISSOs and other security practitioners.	---
2.1.4.b	The Component ISSM shall work directly with the HQ CISO.	---

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

Component ISSMs:

- Oversee the Component information security program
- Ensure that the Component CIO and DHS CISO are kept informed of all matters pertaining to the security of information systems
- Ensure that all communications and publications pertaining to information security, including updates to the 4300 Policies and Handbooks, are distributed to the ISSOs and other appropriate persons within their Component
- Validate all Component information system security reporting
- Consult with the Component Privacy Officer or PPOC for reporting and handling of privacy incidents
- Manage information security resources including oversight and review of security requirements in funding documents
- Test the security of the Component's information systems periodically
- Implement and manage a POA&M process for remediation by creating a POA&M for each known vulnerability
- Ensure that ISSOs are appointed for each Component-managed information system
- Ensure that weekly incident reports are forwarded to the HQ CISO
- Acknowledge receipt of ISVM messages, report compliance with requirements, or notify applicants of the granting of waivers
- Ensure adherence to the DHS Secure Baseline Configuration Guides (Enclosure 1, *DHS 4300A Sensitive Systems Handbook*)
- Develop and publish procedures for implementation of DHS information security policy within the Component

- Implement Department information security policies, procedures, and control techniques to address all applicable requirements
- Ensure training and oversight for personnel with significant responsibilities for information security
 - Oversee the Security Authorization process for the Component's MAs.
 - Maintain an independent Component-wide security control assessment program to ensure a consistent approach to controls effectiveness testing
 - Ensure that an appropriate SOC performs an independent network assessment as part of the security control assessment process for each authorized application
 - Ensure that enterprise security tools are used

2.1.5 Risk Executive

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

All DHS Risk Executives:

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

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

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

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

2.1.6 Authorizing Official

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

Policy ID	DHS Policy Statements	Relevant Controls
2.1.6.a	The DHS CIO shall act as the AO for enterprise information systems or shall designate an AO in writing for DHS mission systems and for multi-component systems without a designated AO.	CA-6
2.1.6.b	The Component CIO shall act as the AO for Component information systems or shall designate an AO in writing all systems without a designated AO.	CA-6
2.1.6.c	Every system shall have a designated AO. (An AO may be responsible for more than one system.)	CA-6
2.1.6.d	The AO shall be responsible for review and approval of any individual requiring administrator privileges. The AO may delegate the performance of this duty to the appropriate system owner or Program Manager.	AC-2
2.1.6.e	The AO shall be responsible for acceptance of remaining risk to organizational operations and assets, individuals, other organizations, and the Nation.	CA-6
2.1.6.f	The AO shall periodically review security status for all systems under his or her purview to determine if risk remains acceptable	CA-6
2.1.6.g	The AO shall perform additional duties in accordance with NIST SP 800-37	CA-6

2.1.7 Security Control Assessor

The Security Control Assessor is a senior management official whose responsibilities include certifying the results of the security control assessment. A Security Control Assessor, who must be a Federal employee, is assigned in writing to each information system by an appropriate

Component official, typically the Component Head or Component CIO. The Security Control Assessor and the team conducting a certification must be impartial. They must be free from any perceived or actual conflicts of interest with respect to the developmental, operational, and or management chains of command associated with the information system; or with respect to the determination of security control effectiveness.

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

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

- The criticality and sensitivity of the information system
- The ultimate risk to organizational operations, organizational assets, and individuals
- The level of assessor independence required for confidence that the assessment results are sound and valid for making credible risk-based decisions.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.7.a	The Component CISO shall serve as Security Control Assessor when no other person has been officially designated.	CA-4
2.1.7.b	A Security Control Assessor may be responsible for more than one system.	CA-4
2.1.7.c	The Security Control Assessor may take the lead for any or all remedial actions.	CA-7
2.1.7d	The Security Control Assessor provides an assessment of the severity of weaknesses or deficiencies in the information systems, and clarifies they prepare the final security assessment report containing the results and findings from the assessment but not making a risk determination.	CA-7

2.1.8 Information Systems Security Officer

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

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

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

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

2.2 Other Roles

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

2.2.1 Secretary of Homeland Security

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

To that end, the Secretary:

- Ensures that DHS implements its Information Security Program throughout the life cycle of each DHS system
- Submits the following to the Director, OMB:
 - the DHS CIO's assessment of the adequacy and effectiveness of the Department's information security procedures, practices, and FISMA compliance
 - the results of an annual independent information security program evaluation performed by the DHS Office of Inspector General (OIG)
 - the Senior Agency Official for Privacy's (SAOP) annual assessment of the Department's privacy policies, procedures, and practices to the Director, OMB

- Provides information security protection commensurate with the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the Department, and on information systems used or operated by the Department, or by a contractor or other organization on behalf of the Department
- Ensures that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the Department’s operations
- Ensures that information security processes are integrated with strategic and operational planning processes to secure the Department’s mission
- Ensures that the Department’s senior officials have the necessary authority to secure the operations and assets under their control
- Delegates authority to the CIO to ensure compliance with applicable information security requirements

2.2.2 Under Secretaries and Heads of DHS Components

The Under Secretaries and Heads of DHS Components are responsible for oversight of their Components’ information security program, including the appointment of CIOs.

Undersecretaries and Heads of Components allocate adequate resources to information systems for information system security.

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

Under Secretaries and the Heads of DHS Components:

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

2.2.3 DHS Chief Information Officer

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

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

The DHS CIO:

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

2.2.4 Component Chief Information Officer

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

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

Component CIOs:

- Establish and oversee their Component information security programs
- Ensure that an AO has been appointed for every Component information system; serves as the AO for any information system for which no AO has been appointed or where a vacancy exists
- Ensure that information security concerns are addressed by Component Configuration Control Boards, Enterprise Architecture Board (EAB), and Acquisition Review Board (ARB)/Investment Review Board (IRB)
- Ensure that an accurate information systems inventory is established and maintained
- Ensure that all information systems acquisition documents, including existing contracts, include appropriate information security requirements and comply with DHS information security policies
- Ensure that System Owners understand and appropriately address risks, including risks arising from interconnectivity with other programs and systems outside their control
- Ensure that an information security performance metrics program is developed, implemented, and funded
- Advise the DHS CIO of any issues regarding infrastructure protection, vulnerabilities or the possibility of public concern
- Ensure that incidents are reported to the DHS SOC within reporting time requirements as defined in this Handbook's Attachment F, "Incident Response and Reporting."
- Work with the DHS CIO and Public Affairs Office in preparation for public release of security incident information. The DHS CIO, or designated representative, has sole responsibility for public release of security incident information.
- Ensure compliance with DHS information systems security policy
- Coordinate and advocate resources for information security enterprise solutions

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

- CBP

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

CIOs of all other Components shall:

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

2.2.5 DHS Chief Security Officer

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

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

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

2.2.6 DHS Chief Privacy Officer

The DHS Chief Privacy Officer is the head of the DHS Privacy Office and is responsible for creation of privacy policies and their implementation in all Components of the Department. The responsibilities of the DHS Chief Privacy Officer include oversight of all privacy activities within the Department, and ensuring compliance with privacy policies.

The DHS Chief Privacy Officer assists Component Privacy Officers and Privacy PPOC with policy compliance at the Component level.

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

The Chief Privacy Officer, as the senior privacy official:

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

2.2.7 DHS Chief Financial Officer

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

Policy ID	DHS Policy Statements	Relevant Controls
2.2.7.a	The DHS CFO shall be the AO for all financial systems managed at the DHS level.	CA-6
2.2.7.b	The DHS CIO has directed that the Component CFO shall be the AO for all financial mission applications managed at the Component level.	CA-6
2.2.7.c	The DHS CFO shall designate the financial systems that fall under the DHS CFO-mandated policy statements.	CA-6
2.2.7.d	The DHS CFO shall publish a comprehensive list of designated financial systems during the fourth quarter of every fiscal year. (This list shall be referred to as the CFO Designated Systems List.)	CA-6

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

2.2.8 Program Managers

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

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

Policy ID	DHS Policy Statements	Relevant Controls
2.2.8.a	Program Managers shall ensure that program POA&Ms are prepared and maintained.	CA-5, PM-4
2.2.8.b	Program Managers shall prioritize security weaknesses for mitigation.	CA-5
2.2.8.c	Program Managers shall provide copies of program POA&Ms to affected System Owners.	CA-5, PM-4
2.2.8.d	<p>Program Managers shall ensure that POA&Ms address the following:</p> <ul style="list-style-type: none"> ▪ known vulnerabilities in the information system ▪ the security categorization of the information system ▪ the specific weaknesses or deficiencies in the information system security controls ▪ the importance of the identified security control weakness or deficiencies ▪ the Component's proposed risk mitigation approach while addressing the identified weaknesses or deficiencies in the security controls the rationale for accepting certain weaknesses or deficiencies in the security controls. 	CA-5

2.2.9 System Owners

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

Policy ID	DHS Policy Statements	Relevant Controls
2.2.9.a	System Owners shall ensure that each of their systems is deployed and operated in accordance with this policy document.	PL-1

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

2.2.10 Common Control Provider

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

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

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

DHS employees, contractors, and others working on behalf of the DHS or its agencies shall follow the appropriate set(s) of rules of behavior.

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

3.0 MANAGEMENT POLICIES

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

3.1 Basic Requirements

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

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

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

Policy ID	DHS Policy Statements	Relevant Controls
3.1.a	Every DHS computing resource (desktop, laptop, server, portable electronic device, etc.) shall be individually accounted for as part of a FISMA ⁴ -Inventoried information system.	CM-8
3.1.b	The Component Chief Information Officer (CIO), in cooperation with each of the Component's senior officials, shall be responsible for ensuring that every DHS computing resource is identified as an information system or as a part of an information system, either as an MA or as a general support system (GSS).	CM-8
3.1.c	The System Owner or designee shall develop and maintain a Security Plan (SP) for each information system. Component Authorizing Officials (AO) shall review and approve SPs.	PL-2
3.1.d	An ISSO shall be designated for every information system and serve as the point of contact (POC) for all security matters related to that system.	PL-1

⁴ FISMA: Federal Information Security Management Act, 44 U.S.C. 3541

Policy ID	DHS Policy Statements	Relevant Controls
3.1.e	Component information security programs shall be structured to support DHS and applicable FISMA, Office of Management and Budget (OMB), and other Federal requirements.	PL-1
3.1.f	Information security reports regarding DHS systems shall be submitted to the Senior Component official or designated representative.	---
3.1.g	Component CISOs/ISSMs shall ensure that their information systems comply with the DHS Enterprise Architecture (EA) Technical Reference Model (TRM) and Security Architecture (SA) or maintain a waiver, approved by the DHS CIO/ CISO.	PL-1, PM-1
3.1.h	The DHS CISO shall issue Department-wide information security policy, guidance, and information security architecture requirements for all DHS systems.	CM-2, CM-6
3.1.i	Component CISOs shall implement DHS information security policies, procedures, and control techniques to meet all applicable requirements.	PL-1, PM-1
3.1.j	Component CISOs shall develop and manage information security guidance and procedures unique to Component requirements.	PL-1, PM-1
3.1.k	Security-relevant management processes and tools shall comply with applicable NIST-standard protocols and conventions as described in NIST SP 800-126, <i>The Technical Specification for the Security Content Automation Protocol (SCAP)</i> , including the Common Platform Enumeration (CPE), Common Configuration Enumeration (CCE), and Common Vulnerabilities and Exposures (CVE)	RA-5, SI-2, CM-6

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

3.2 Capital Planning and Investment Control

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

Information security is a business driver and any risks found through security testing are ultimately business risks. Information security personnel should be involved to the maximum extent possible in all aspects of the acquisition process, including drafting contracts, and procurement documents. DHS Management Directive (MD) 102-01, "Acquisition Management Directive" and DHS MD 4200.1, "IT Capital Planning and Investment Control (CPIC) and

Portfolio Management” provide additional information on these requirements. Consult the DHS CPIC Guide for more information.

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

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

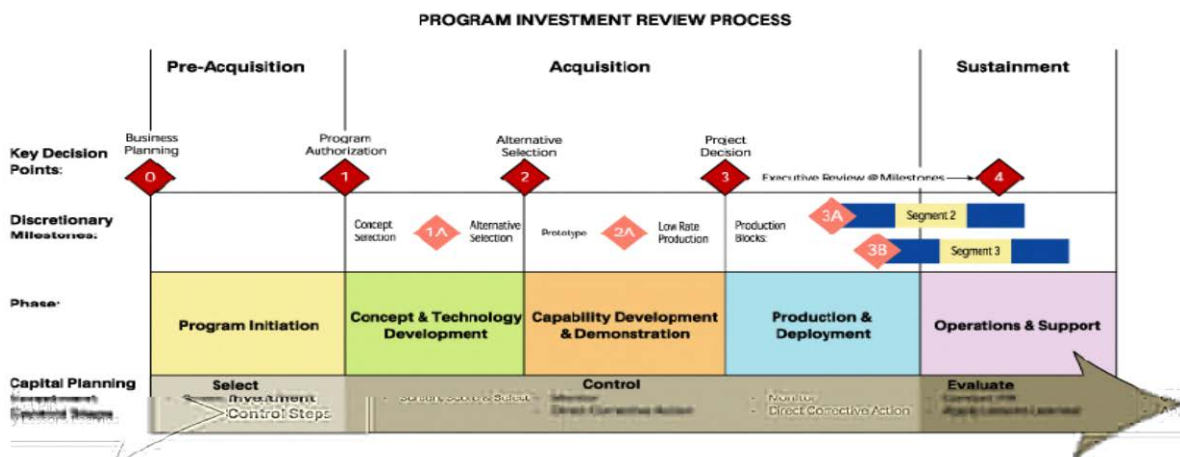
Policy ID	DHS Policy Statements	Relevant Controls
3.2.a	System Owners shall include information security requirements in their CPIC business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP) for each DHS system.	PM-3, PM-11, SA-1
3.2.b	System Owners or AOs shall ensure that information security requirements and Plans of Action and Milestones (POA&M) are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.	PM-3, PM-4, SA-2
3.2.c	Component IRBs/ARBs ⁵ shall not approve any capital investment in which the information security requirements are not adequately defined and funded.	PM-3, SA-2
3.2.d	The DHS CISO shall perform security reviews for planned information system acquisitions over \$2.5 million, and in selected additional cases.	SA-1
3.2.e	Components shall ensure that information security requirements as described in this Policy Directive are met in the acquisition of all DHS systems and services used to input, process, store, display, or transmit sensitive information.	SA-4
3.2.f	Procurement authorities throughout the Department shall enforce the provisions of the Homeland Security Acquisition Regulation (HSAR).	SA-1, SA-4
3.2.g	Procurements for services and products involving facility or system access control shall be in accordance with DHS guidance regarding HSPD-12 implementation.	

⁵ IRB: Investment Review Board; ARB: Acquisition Review Board

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

3.2.1 Capital Planning and Investment Control Process

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



Error! Not a valid bookmark self-reference. illustrates how each KDP relates to its respective CPIC and SELC phase.

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

- Designated as a Level 1 acquisition
- Directed to charter a major acquisition Integrated Product Team (IPT)
- Entered into the budget process (Typically the Fiscal Year +2 budget)
- Authorized to move to the Concept & Technology Development phase

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

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

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

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

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

3.3 Contractors and Outsourced Operations

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

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

System Owners and Project Managers must review and include security requirements in solicitation documents *prior to the acquisition of information systems or services*. Information security must be a key factor in the source selection process and must be weighed against the sensitivity and criticality of the data to be processed. If the solicitation includes purchase of a commercial off-the-shelf (COTS) application or if the system being developed has a COTS element, the security aspects of the COTS product must be considered.

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

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

Contractors and Outsourced Operations Responsibilities
<p>Component CISOs/ISSMs</p> <p>Establish and maintain a contractor and outsourced operations policy for the Component</p> <p>System Owners/ Project Managers</p>

Contractors and Outsourced Operations Responsibilities
Ensure that computer security requirements are reviewed and included in all applicable statements of work and other contractual agreements throughout the System Life Cycle
Ensure that basic security requirements are integrated into the software and procurement life cycle for project development
Ensure that computer security requirements are specified in the system design and functional requirements documents, and in other SELC documents, as required
ISSOs
Coordinate with the System Owners to ensure that contractor and outsourced operations policy requirements are met

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

3.4 Performance Measures and Metrics

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

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

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

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

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

A security metrics program includes four interdependent elements:

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

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

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

3.5 Continuity Planning for Critical DHS Assets

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

- Continuity of Operations Planning (COOP)

- Contingency Planning (CP)
-

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

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

3.5.1 Continuity of Operations Planning

DHS must have the capability to ensure continuity of essential functions under all circumstances. COOP policies are designed to establish a Department-wide capability to react to emergency events (**response**); to restore essential business functions (**recovery**); and to resume normal operations (**reconstitution**).

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

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

Policy ID	DHS Policy Statements	Relevant Controls
3.5.1.a	When available, a DHS-wide process for continuity of operations (CO) planning shall be used in order to ensure continuity of operations under all circumstances.	CP-2
3.5.1.b	Components shall develop, test, implement, and maintain comprehensive Continuity of Operations Plans (COOP) to ensure the recovery and continuity of essential DHS functionalities.	CP-2, CP-4
3.5.1.c	All CISOs/ISSMs shall ensure that all COOPs under their purview are tested and exercised annually.	CP-4
3.5.1.d	All Chief Financial Officer (CFO)- Designated Systems requiring high availability shall be identified in COOP plans and exercises.	CP-1

Policy ID	DHS Policy Statements	Relevant Controls
3.5.1.e	All personnel involved in COOP efforts shall be identified and trained in the procedures and logistics of COOP development and implementation.	AT-3, CP-3
3.5.1.f	To ensure that accounts can be created in the absence of the usual account approval authority, systems that are part of the Critical DHS Assets Program shall have provisions to allow a Component CISO/ISSM or Component CIO to approve new user accounts as part of a COOP scenario.	AC-2
3.5.1.g	Each Component shall compile and maintain a list of mission-critical information systems in support of COOP.	CM-8, CP-1
3.5.1.h	The DHS and Component CISOs/ISSMs shall ensure preparation and maintenance of plans and procedures to provide continuity of operations for information systems.	CP-1
3.5.1.i	DHS information systems that are part of the DHS Continuity Planning for Critical DHS Assets Program shall be provided requirements for system-level contingency planning by a Component Contingency Planning Program Office or by a DHS Contingency Planning Program Office.	---

General COOP planning responsibilities are provided in the following table.

Continuity of Operations Planning Responsibilities
<p>DHS Continuity Planning Program Director</p> <ul style="list-style-type: none"> Administers the continuity planning for critical assets program Develops, maintains, and promulgates program requirements Provides oversight and ensures program compliance across DHS Provides COOP guidelines to Components Facilitates development and testing of COOP plans Approves COOP plans and maintains COOP status <p>Component CISOs/ISSMs</p> <ul style="list-style-type: none"> Identify and align office functions with DHS essential functions Identify vital records, information systems, and personnel requirements needed to recover office functions

Continuity of Operations Planning Responsibilities
Administer the Component Continuity Planning program
Ensure the development of the Component's COOPs
Ensure that COOPs are implemented for each line of business
Provide COOP status and strategy to the DHS Continuity Planning Program Director
Develop and maintain a Component COOP Multi-Year Strategy and Program Plan
Component ISSOs
Comply with the Component COOP program
Perform continuity planning and testing and document results
Assist in development of the Component COOP Multi-Year Strategy and Program Plan
Ensure that operational security is maintained during any test or recovery activities

Component ISSOs**3.5.1.1 COOP Requirement**

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

3.5.1.2 COOP Objectives

A COOP is designed to achieve the following objectives:

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

3.5.1.3 COOP Plan Content

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

- Essential functions (including information systems requirements, vital records and databases, and functional recovery activities)

- Essential personnel
- Alternate operating facilities
- Interoperable communications
- Human capital issues (inclusion of occupant emergency planning)
- Devolution of control (delegations of authority and orders of succession)
- Reconstitution (return to normal operations)

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

3.5.1.4 COOP Test, Training, and Exercise

The most important aspect of a successful COOP is the periodic testing and exercising of the plan. Personnel should be trained and plans must be tested periodically. Tests and exercises serve to validate specific aspects of plans, policies, procedures, systems, and facilities that would be used during an emergency. DHS Components must conduct periodic tests so that weaknesses can be identified and corrected. Results must be documented.

3.5.2 Contingency Planning

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

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

Policy ID	DHS Policy Statements	Relevant Controls
3.5.2.a	The DHS CIO shall provide guidance, direction, and authority for a standard DHS-wide process for contingency planning for information systems.	CP-1
3.5.2.b	System Owners shall develop and document information system Contingency Plans (CPs) for their programs, manage plan changes, and distribute copies of the plan to key contingency personnel. Component CIOs shall review and approve Component-level information system CPs.	CP-1, CP-2
3.5.2.c	Components shall ensure implementation of backup policy and procedures for every Component information system.	CP-9
3.5.2.d	The DHS CIO shall ensure that each DHS system has contingency capabilities commensurate with the <i>availability</i> security objective. The minimum	CP-1

Policy ID	DHS Policy Statements	Relevant Controls
	<p>contingency capabilities for each impact level are as follows:</p> <p>High impact – System functions and information have a high priority for recovery after a short period of loss.</p> <p>Moderate impact – System functions and information have a moderate priority for recovery after a moderate period of loss.</p> <p>Low impact – System functions and information have a low priority for recovery after prolonged loss.</p>	
3.5.2.e	<p>CPs shall be developed and maintained by all DHS Components in accordance with the requirements for the FIPS 199 potential impact level for the availability security objective. These plans shall be based on three essential phases: Activation/Notification, Recovery, and Reconstitution. Components shall review the CP for the information system at least annually and revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.</p>	CP-1, CP-2
3.5.2.f	<p>The DHS CIO shall ensure that CP testing is performed in accordance with the availability security objective. The minimum contingency testing for each impact level follows:</p> <p>High impact – System recovery roles, responsibilities, procedures, and logistics in the CP shall be used within a year prior to authorization to recover from a simulated contingency event at the alternate processing site. The system recovery procedures in the CP shall be used at least annually to simulate system recovery in a test facility.</p> <p>Moderate impact – The CP shall be tested at least annually by reviewing and coordinating with organizational elements responsible for plans within the CP. This is achieved by performing a walk-through/tabletop exercise.</p> <p>Low impact – CP contact information shall be verified at least annually.</p>	CP-4, CP-7
3.5.2.g	<p>The DHS CIO shall ensure that contingency training is performed in accordance with the availability security objective. The minimum contingency planning for each impact level follows:</p> <p>High impact – All personnel involved in contingency planning efforts shall be identified and trained in their contingency planning and implementation roles, responsibilities, procedures, and logistics. This training shall incorporate simulated events. Refresher training shall be provided at least annually.</p> <p>Moderate impact – All system personnel involved in contingency planning efforts shall be trained. Refresher training shall be provided at least annually.</p> <p>Low impact – There is no training requirement.</p>	CP-3
3.5.2.h	<p>Components shall coordinate CP testing and/or exercises as appropriate, using COOP-related plans for systems with moderate and high availability FIPS-199 categorization.</p>	CP-4

Contingency planning responsibilities are provided in the following table.

Contingency Planning Responsibilities

DHS Continuity Planning Program Director

Administers Continuity Planning for Critical DHS Assets Program.

Develops, maintains, and promulgates program requirements

Provides oversight and ensures program compliance across DHS Components

Provides contingency planning guidelines to Component CISOs/ISSMs

Facilitates the development and testing of Contingency Plans

Approves DHS Contingency Plans and maintains status

System/Network Administrators

Participate in all phases of the contingency planning process

Site Managers/System Owners

Ensure that the system's FIPS 199 potential impact for the availability security objective is correct and maintained to be consistent with system information processing changes

Ensure that adequate resources are budgeted for contingency planning, testing, and training consistent with the availability objective of the system

Ensure that adequate contingency plans are included in Security Authorization process documentation

Component CISOs/ISSMs

Establish Component continuity planning programs consistent with Department policy

Provide contingency planning status and strategy to the DHS Continuity Planning Program Director

Component ISSOs

Comply with the Component continuity planning program

Ensure that the system's FIPS 199 potential impact for the availability security objective is consistent with the information types processed, stored, and transmitted by the system

Ensure comprehensive contingency plans are developed, as required, for each major application and general support system under their purview

Perform contingency planning, testing/exercising, and training, as required.

Ensure operational security is maintained during any test or recovery activities

3.5.2.1 Contingency Planning Requirement

Requirements for implementation of contingency planning are found in

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

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

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

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

- NIST SP 800-53, Rev 3, “Recommended Security Controls for Federal Information Systems and Organizations,” August 2009, with updated errata May 01, 2010”

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

3.5.2.2 Contingency Plan Development

Contingency planning is designed to achieve the following objectives:

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

3.5.2.3 Contingency Plan Format and Content

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

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

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

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

3.5.2.4 Contingency Plan Test and Exercise

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

3.5.2.5 Contingency Plan Training

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

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

3.6 System Engineering Life Cycle

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

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

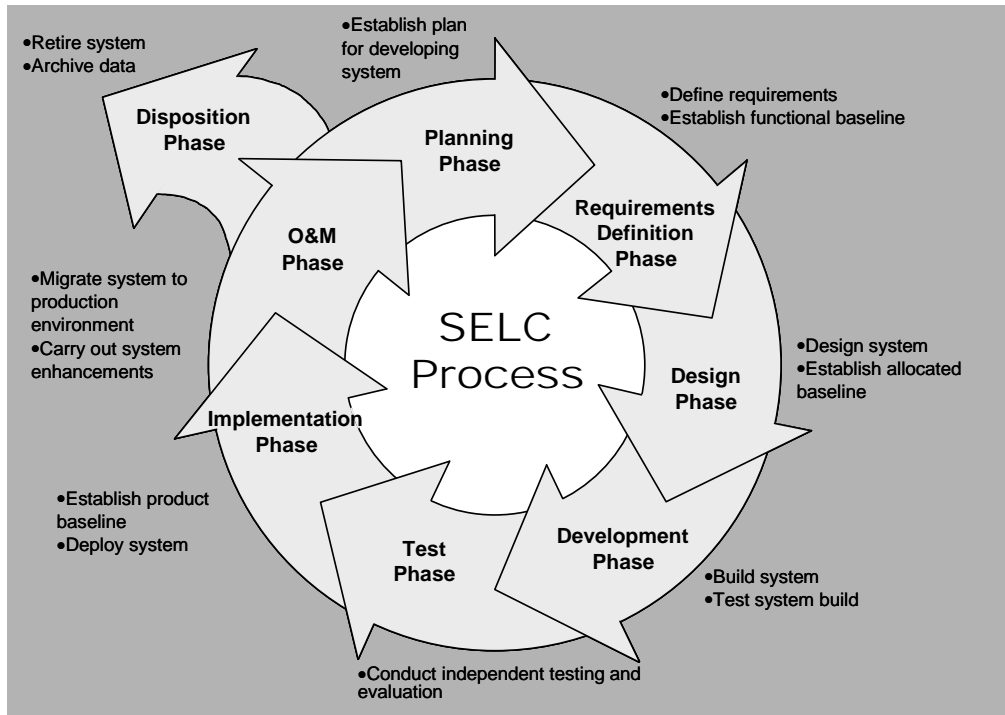


Figure 1 – The SELC process

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

SELC responsibilities are provided in the following table.

SELC Responsibilities
<p>DHS CIO</p> <p>Defines and promulgates the SELC process</p> <p>Ensures that information security life cycle planning is integrated into capital planning and investment</p>

SELC Responsibilities
control processes
DHS CISO
Ensures that information security requirements are included in the SELC
Oversees proper implementation of security controls in system development
Component CISOs/ISSMs
Establishes procedures for reviewing compliance with SELC documentation requirements
Participates in capital planning and investment management meetings involving SELC considerations for systems and networks
Ensures that required information security documentation is produced and reviewed in accordance with SELC milestones
Approves information security documentation produced as part of the SELC process (except the Security Authorization Process package)
ISSOs
Participates in planning and executing the SELC process
Provides information security expertise to system development teams
Reviews and comments on all SELC security documents
System Owners/Project Managers
Ensure required security documents and reviews are included in the SELC
Ensure that adequate funding is available for implementation of security requirements
Prepare required security documents

3.6.1 Planning

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

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

3.6.2 Requirements Definition

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

- Updating the Risk Assessment and Security Plan
- Reviewing Baseline Security Requirements

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

3.6.3 Design

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

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

3.6.4 Development

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

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

3.6.5 Test

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

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

3.6.6 Implementation

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

- Conducting the Operational Security Control Assessment on upgraded or new systems
- Reviewing adequacy of budget requirements
- Finalizing the security inputs in the Training Plans
- Updating the Risk Assessment and Security Plan
- Finalizing the Security Authorization package

3.6.7 Operations and Maintenance

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

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

3.6.8 Disposition

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

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

3.7 Configuration Management

Configuration Management (CM) includes management of all hardware and software elements of information systems and networks. CM within DHS consists of a multi-layered structure – policy,

procedures, processes, and compliance monitoring. Each Component shall use an appropriate level of configuration management.

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

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

Configuration management has security implications in three areas:

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

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

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

Policy ID	DHS Policy Statements	Relevant Controls
3.7.a	Components shall develop and maintain a configuration management plan (CMP) for each information system as part of its SP. All DHS systems shall be under the oversight of the officer responsible for Configuration Management.	CM-1, CM-9
3.7.b	Components shall establish, implement, and enforce configuration management controls on all information systems and networks and address significant deficiencies as part of a POA&M.	CA-5, CM-3, PM-4
3.7.c	Information security patches shall be installed in accordance with	SI-2

Policy ID	DHS Policy Statements	Relevant Controls
	configuration management plans and within the timeframe or direction stated in the Information Security Vulnerability Management (ISVM) message published by the DHS Enterprise Operations Center (SOC).	
3.7.d	System Owners shall document initial system configuration in detail and shall control all subsequent changes in accordance with the configuration management process.	CM-2, CM-3, CM-9
3.7.e	Workstations shall be configured in accordance with DHS guidance on the U.S Government Configuration Baseline (USGCB) (formerly known as the Federal Desktop Core Configuration [FDCC]). Configuration shall include installation of the DHS Common Policy Object Identifier (OID), Common Policy Framework Root CA certificate, and the DHS Principal CA certificate.	CM-2, CM-6, CM-9
3.7.f	Components shall monitor USGCB (or DHS-approved USGCB variant) compliance using a (NIST)-validated Security Content Automation Protocol (SCAP) tool.	---
3.7.g	The System Owner shall request an exception for information systems that use operating systems or applications that are not hardened or do not follow configuration guidance identified in Enclosure 1 of <i>DHS Sensitive Systems Handbook</i> DHS Secure Baseline Configuration Guides. Requests shall include a proposed alternative secure configuration.	CM-2, CM-6
3.7.h	Components shall ensure that CM processes under their purview include and consider the results of a security impact analysis when considering proposed changes.	CM-4

Configuration management responsibilities are provided in the following table.

Configuration Management Responsibilities
<p>Component CISOs/ISSMs Ensure that security issues are being addressed in configuration reviews and by Change Control Boards</p> <p>Security Control Assessors Re-assess the system if significant configuration changes have been made</p> <p>AOs Re-authorize systems if significant configuration changes have been made Ensure that Project Managers and Development/O&M Support Teams implement an effective CM process in accordance with SELC requirements</p>

Configuration Management Responsibilities

Project Managers/ISSOs

Ensure that CM procedures are documented and implemented for all proposed configuration changes to information systems

Ensure that all proposed configuration changes to operating systems and applications are analyzed prior to implementation to determine if the proposed change has security implications

Maintain a capability to quickly approve and implement time-sensitive security patches in reaction to late-breaking security vulnerabilities identified by the DHS SOC

Ensure that all proposed configuration changes to operating systems, operating system security features, applications, critical system files, and system devices are formally approved, tested, and documented prior to the change being implemented

Ensure that all approved changes to the configuration baseline are documented, reviewed for accuracy, and that records are maintained for each system for both the current and all previous configurations

Ensure that formal system configuration reviews are performed

Ensure that accurate system documentation and configuration logs are maintained to reflect current and prior configuration baselines

Prepare and distribute a CM plan for each system under their authority

Implement and enforce CM controls

Project Team

Understand and comply with the system CM plan

Comply with CM controls and procedures

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

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

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

The CM process continues throughout the system life cycle.

3.8 Risk Management

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

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

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

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

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

Risk management responsibilities are provided in the following table.

Risk Management Responsibilities

DHS CISO

Establishes and enforces policy relating to the risk management process

Security Control Assessor

Evaluates the risk assessment document as part of the assessment process

Ensures that the risk assessment document contains information required for the Security Authorization Process

Informs the AO of the possible mitigation actions for residual risks

AOs

Determine the overall degree of acceptable risk based on the Component's mission requirements

Determine whether residual risks are within tolerable limits

Make a risk-based decision to grant a system Authority to Operate (ATO) or Interim Authority to Operate (IATO); or to deny system authorization because the risks are beyond an acceptable level

System Owners

Assist in determining the degree of acceptable residual risk based on the Department's mission requirements

Review the assessment package and ensure resources are provided to implement risk mitigation measures

Project Managers/ISSOs

Conduct the initial risk assessment

Ensure that the SP and risk assessment contain information required by assessment activities and address all appropriate management, operational, and technical controls

Initiate follow-on risk assessments if any significant changes to the system configuration or to the operational or threat environment have occurred, or every three (3) years, whichever comes first

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

- Risk assessment
- Risk mitigation
- Evaluation and assessment

3.8.1 Risk Assessment

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

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

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

3.8.2 Risk Mitigation

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

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

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

3.8.3 Evaluation and Assessment

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

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

3.9 Security Authorization and Security Assessments

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

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

Type Security Authorization Process shall consist of a master Security Authorization Process package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites.

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

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

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

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

Authorization is the official management decision that permits the operation of a system. It includes explicitly accepting the risk to Department operations, assets, or individuals, based on the implementation of an agreed-upon set of security controls. The AO accepts security responsibility for the operation of an assessed system and officially grants Authority to Operate (ATO). AOs shall be identified in TrustedAgent FISMA (TAF). The Component CIO shall serve as the AO for any system where an AO has not been appointed or where a vacancy exists.

A common controls approach (type authorization) may be used for authorizing systems. Attachment D to this Handbook, *Type Authorization*, provides specific guidance. The AO must approve the use of any common controls-based Security Authorization Process.

Components shall categorize systems in accordance with FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems” and shall apply the appropriate NIST SP 800-53 controls. The Risk Management System (RMS) automated tool shall be used to produce Security Authorization Process packages. Artifacts generated during the Authorization process shall be uploaded into TAF). TAF supports the POA&M process and generates quarterly reports and annual self-assessments.

NIST SP 800-37 describes the six Security Authorization Process steps which are listed below:

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

The DHS “Security Authorization Process Guidance for SBU Systems: Users Manual” provides detailed instructions for creating authorization artifacts, using authorization tools for authorizing systems, and the timeline for creating authorization artifacts, tracking remediation activities, and performing the required self-assessments and generating the required reports.

All Security Authorization Processes shall be completed in accordance with “DHS 4300A Sensitive Systems Policy Directive” for unclassified systems and “DHS 4300B National Security Systems Policy Directive” for collateral systems. Sensitive Compartmented Information (SCI) Systems shall be authorized by the DHS Office of Intelligence and Analysis (DHS I&A).

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

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

Policy ID	DHS Policy Statements	Relevant Controls
3.9.a	Components shall assign an impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability) for each DHS information system. Components shall apply NIST SP 800-53 controls as tailored specifically to the security objective at the determined impact level in the Attachment M to <i>DHS 4300A, Sensitive Systems Handbook</i> , “Tailoring the	PM-10, RA-2

Policy ID	DHS Policy Statements	Relevant Controls
	NIST 800-53 Security Controls.”	
3.9.b	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 FIPS 199 impact level established for each separate security objective (confidentiality, integrity, availability).	---
3.9.c	It is recommended that Components pursue <i>Type Security Authorization Process</i> for information resources that are under the same direct management control; have the same function or mission objective, operating characteristics, security needs, and that reside in the same general operating environment, or in the case of a distributed system, reside in various locations with similar operating environments. <i>Type Security Authorization Process</i> shall consist of a master <i>Security Authorization Process</i> package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites.	---
3.9.d	The AO for a system shall be identified in Trusted Agent FISMA (TAF). The Component CIO shall serve as the AO whenever the System Owner or an appropriate program official has not been named as the AO.	---
3.9.e	Component CISOs shall ensure that all information systems are formally assessed through a comprehensive evaluation of their management, operational, and technical security controls.	CA-2, PM-10
3.9.f	As part of the authorization process, a supporting assessment shall determine the extent to which a particular design and implementation plan meets the DHS required set of security controls.	PM-10
3.9.g	Component CISOs/ISSMs shall ensure that a risk assessment is conducted whenever modifications are made to sensitive information systems, networks, or their physical environments, interfaces, or user community. SPs shall be updated and re-authorized if warranted.	PM-9, RA-3
3.9.h	Components shall authorize systems at Initial Operating Capability (IOC) and every three (3) years thereafter, or whenever a major change occurs, whichever occurs first. An Authority to Operate (ATO) of six (6) months or less shall receive an ATO authorization period waiver from the DHS CISO before submission to the AO for a final authorization decision.	CA-6, PM-10
3.9.i	AOs may grant an Interim Authorization to Operate (IATO) for systems that are undergoing development testing or are in a prototype phase of development. A system shall be assessed and authorized in an ATO letter prior to passing the Acquisition Decision Event 2C milestone in the SELC. IATOs shall not be used for operational systems. The AO may grant an IATO	PL-1, PM-10

Policy ID	DHS Policy Statements	Relevant Controls
	for a maximum period of 6 (six) months and may grant 1 (one) 6 (six) month extension. Systems under an IATO shall not process sensitive information but may attach to system networks for testing.	
3.9.j	If the system is not fully authorized and has not received a full ATO by the end of the second and final IATO, the system shall not be deployed as an operational system.	PL-1, PM-10
3.9.k	Components shall request concurrence from the DHS CISO for all authorizations for 6 (six) months or less.	---
3.9.l	The DHS CISO shall specify tools, techniques, and methodologies used to assess and authorize DHS information systems, report and manage FISMA data, and document and maintain POA&Ms.	CA-1, PM-4
3.9.m	Currently, all DHS systems shall be authorized using the automated tools, TAF and Risk Management System (RMS), which have been approved by the DHS CISO.	CA-1, CA-2, PM-10
3.9.n	The DHS CISO shall maintain a repository for all Security Authorization Process documentation and modifications.	CA-1
3.9.o	Component CISOs shall establish processes to ensure that the Security Authorization Process is used consistently for all Component systems.	CA-1, PM-10
3.9.p	System Owners shall use the POA&M process to manage vulnerabilities, correct deficiencies in security controls, and remediate weaknesses in SPs.	CA-5, PM-4
3.9.q	The AO shall formally assume responsibility for operating an information system at an acceptable level of risk. System operation with sensitive information is prohibited without an ATO.	CA-6, PM-10
3.9.r	ATOs shall only be provided for systems that fully comply with policy or have been granted appropriate exceptions or waivers.	CA-6, PM-10
3.9.s	Artifacts in support of <i>new</i> ATOs shall not be older than 13 months. Older artifacts remain valid during the life of a current ATO.	---
3.9.t	The DHS CIO may revoke the ATO of any DHS information system.	CA-6
3.9.u	The Component CIO may revoke the ATO of any Component-level information system.	CA-6
3.9.v	Components shall assign a common control provider to share controls between systems (e.g., at hosting centers). The authorization package of those common	

Policy ID	DHS Policy Statements	Relevant Controls
	controls must be shared with those operating under the controls.	
3.9.w	DHS enterprise services shall be required to provide a catalog of common controls that have been assessed and authorized by the AO of that service.	---
3.9.x	An Enterprise System Security Agreement (ESSA) shall be developed for all enterprise services.	---

Assessment and Authorization responsibilities are provided in the following table.

Assessment and Authorization Responsibilities
<p>DHS CISO Establishes and enforces policy relating to the Security Authorization Process</p> <p>Security Control Assessor Ensures that the SP, Security Control Assessment, Contingency Plan, and Risk Assessment contain the information required for Security Authorization Process Prepares the assessor’s statement, which reflects the state of the security controls, based on the results of the Security Control Assessment Recommends to the AO the possible implementation of additional risk mitigation actions that would mitigate the residual risks identified by the Security Control Assessment Assembles the assessment package that includes the assessment findings, and transmit to the AO Maintains files of assessment packages for each system</p> <p>AOs Determine degree of acceptable residual risk based on Department’s mission requirements Review the state of the security controls for the system and the Department’s mission requirements Assess the correctness and effectiveness of security controls and identify the level of residual risk for the system Determine whether the residual risk is within tolerable limits Make a risk-based decision to (1) grant system authorization, (2) grant an IATO for a designated period of time (no longer than 6 months - systems in development testing or prototypes only), or (3) deny system authorization.</p> <p>System Owners Assessment Responsibilities: Ensure that adequate resources are budgeted for and allocated to the Security Authorization Process. Review the results of the Initiation and Security Assessment phases and ensure that resources are</p>

Assessment and Authorization Responsibilities

provided to identify and implement risk mitigation measures.

Authorization Responsibilities:

Assist in determining degree of acceptable residual risk based on Department's mission requirements

Review the Assessment Package and ensure that resources are provided to implement risk mitigation measures

Project Managers/ISSOs

Ensure that the RMS automated tool is used to develop Security Authorization Process packages

Assessment Responsibilities:

Ensure that the Security Plan and Risk Assessment contain information required by assessment activities

Develop the Security Control Assessment plan, conduct the Security Control Assessment, and prepare the Security Control Assessment Report (the Security Assessment Report (SAR)).

Authorization Responsibilities:

Complete the final Risk Assessment, update the Security Plan, prepare the assessment findings, and prepare a Draft Assessment Statement.

Complete the Assessment Package and forward to the Security Control Assessor.

Maintain files of the Assessment Package.

Initiate re-authorization activities if any significant changes to the system configuration or to the operational/threat environment that might affect system security have occurred, or every three (3) years, whichever comes first.

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

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

The controls required to support the security objective for an information system shall be implemented. There is no requirement to implement extra controls beyond this minimum standard, but any program may implement additional or more stringent controls. This policy amplification is a Department-level risk-based decision that is consistent with the FISMA requirement to "cost-effectively reduce information security risks to an acceptable level." The tailoring of controls and use of compensating controls is also consistent with providing the safeguards necessary to reduce the risks in a specific operational environment.

This policy amplification is also consistent with the NIST information security guidance which promulgates the "concept of risk based decisions." The due diligence required by FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems" of determining the exact impact level each type of information on the system, and each of the security objectives, will lead to well defined impact levels for confidentiality, integrity, and

availability of the system as a whole. It is important, when using a risk-based decision to minimize the security controls, that all of the information and the risks to that information be clearly defined and documented so that the AO can make an informed decision on the level of risk that is acceptable for the system and its information in the specific operational environment.

The “DHS FIPS 199 Workbook” stipulates impact levels (high, moderate, low) to be assigned to each security objective. Under these categories, a system with low risk availability, high risk integrity, and low risk confidentiality is not required to implement all high controls across the board, rather the controls that fall out of the analysis shall be implemented (i.e., high levels for integrity controls, low for the confidentiality and availability controls).

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

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

Attachment M to this Handbook, “Tailoring the NIST SP 800-53 Security Controls,” lists the NIST SP 800-53 controls by impact level and by security objective, and provides information on the possible tailoring of these controls and the use of compensating controls.

3.9.2 Privacy Impact Assessment

Information systems involving PII are required to have a Privacy Impact Assessment (PIA).⁶ A Privacy Threshold Analysis (PTA) is first performed to determine whether potential privacy or PII data is being processed or stored. Systems that are determined to have privacy concerns require a formal PIA. See Section 3.14, Privacy and Data Security for additional information.

3.9.3 E-Authentication

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

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

The E-Authentication Workbook and instructions are available on the DHS CISO Web page. The DHS Compliance Help Desk (202) 357-6100 can also provide assistance in obtaining these documents.

3.9.4 Risk Assessment

Risk Assessment is the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this

⁶ Section 208 of the E-Government Act

impact. An initial risk assessment is used to understand the unique system risks and to determine if any controls are required to address specific threats or weaknesses. The initial assessment incorporates system characterization information, security categorization, PTA and PIA, and e-Authentication assessment. The results will be used to directly address the controls that will be documented in the Security plan and implemented in the system.

An initial Risk Assessment document is generated within RMS whenever a Security Authorization Process package is initiated.

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

DHS follows the overall risk process as described in NIST Special Publication 800-30, “{Risk Management Guide for IT Systems.”

The DHS *Security Authorization Process Guidance for SBU Systems: Users Manual* provides detailed information on developing Risk Assessments within RMS.

3.9.5 Security Plan

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

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

3.9.6 Contingency Plan

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

- For systems with a **low impact for availability**, the System Owner may determine the Contingency Plan format and content that is appropriate for the system and its environment. The Contingency Plan generated in RMS may also be used.
- For systems with a **moderate impact level for availability**, the default Contingency Plan template in RMS should be used.
- Systems with a **high impact level for availability** should develop a rigorous Contingency Plan. The DHS-developed high impact version of a contingency plan, “IT Contingency and Disaster Recovery Plan,” should be used. This template is found in the Additional

Documents section of RMS. The high impact plan can be received in RMS when creating a package, by answering “Yes” to additional documents in the questionnaire. This template is also available in this Handbook’s Attachment K, “IT Contingency Plan Template.”

The DHS “Security Authorization Process Guidance for SBU Systems: Users Manual” provides detailed information on developing the Contingency Plan within RMS.

3.9.7 Security Control Assessment Plan

The Security Control Assessment Plan outlines the methodology for testing and verifying that the management, operational, and technical controls are in place and operating as expected. The Security Control Assessment Plan template within RMS provides starting point for developing the plan.

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

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

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

3.9.8 Contingency Plan Testing

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

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

3.9.8.1 Systems with High Impact Availability — *Testing Required*

Components shall ensure that an established alternate site is available for systems with high impact availability. Resources for establishing an alternate site shall be identified and made available for systems assessed as high impact for availability.

For systems with high impact availability, a full-scale test of the Contingency Plan is preferred. In a full-scale test, the triggering incident shall be simulated, but the detection, containment, and recovery steps shall be executed in accordance with the plan. This test shall include coordination with the alternate site. The following objectives shall be achieved:

1. The test demonstrates that the system can be brought to an operational condition at the designated alternate site by following the procedures and instructions described in the plan.

2. It is important that the plan draw only on resources that are normally located away from the site where the incident occurs.
3. The test verifies that the organizational units responsible for the Contingency Plan fully understand their responsibilities and are able to carry them out in a timely manner.
4. The test verifies that the system is brought to an operational condition within the allotted recovery time.
5. The test verifies that system information is restored to the expected state, so that operations can resume in a synchronized manner.
6. The test verifies that access to system information by authorized business area personnel has been reestablished.

In circumstances that preclude a full-scale test, a rigorous tabletop exercise with a planned follow-on for a full test shall provide an acceptable alternative. The tabletop exercise is described below in the section on moderate impact systems.

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

For systems with moderate impact availability, a full-scale test of the Contingency Plan shall be encouraged, but is not required. A tabletop exercise shall be acceptable for most moderate impact systems. The most important elements are that the actual individuals involved in the recovery process are involved in the exercise and that the exercise formally addresses all of the steps in the plan. The following objectives shall be achieved.

1. The exercise walks through the procedures and instructions described in the Contingency Plan.
2. Results for each step are simulated as rigorously as possible.
3. The exercise makes reference only to personnel and other resources that will be located away from the site where the incident occurs.
4. The exercise requires each organizational unit to explain how they would carry out their responsibilities.
5. A timeline with reasonable times for events is used to illustrate that the system could be brought to an operational condition within the allotted system recovery time.
6. The exercise illustrates how access to system information by authorized business area personnel would be reestablished.
7. The entire exercise is used as a tool to train the teams involved on their responsibilities during an emergency.

In a tabletop exercise, the triggering incident, detection, containment, and recovery are simulated. The Contingency Plan shall be used to walk through a prepared scenario in order to demonstrate how system recovery would be achieved. This exercise shall include personnel from the site(s) where the system would be recovered.

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

For systems whose availability is categorized as low impact, Contingency Plan testing is optional. At a minimum, the plan shall be reviewed and evaluated for feasibility every two years or whenever significant changes are made to the system. A memo shall be developed that indicates that “the system is a FIPS 199 low impact system; therefore, the system’s Contingency Plan is not required to be tested.”

The DHS *Security Authorization Process Guidance for SBU Systems: Users Manual* provides detailed information on developing the Security Control Assessment Plan within RMS.

3.9.9 Security Assessment Report

The Security Assessment Report (SAR) summarizes the results of the Security Control Assessment and the system’s compliance with the defined security controls in the SP. The findings should state whether or not the system is fully compliant with the SP and Risk Assessment. If the testing finds that the system is compliant, but residual risk remains, the SAR must document these risks. Security Control Assessment results are attached to support the findings in the SAR.

A SAR template is available in RMS. The DHS *Security Authorization Process) Guidance for SBU Systems: Users Manual* provides detailed information on developing the SAR within RMS.

3.9.10 Plan of Action and Milestones

The POA&M is part of the authorization package. The POA&M documents the weaknesses that will be mitigated and the corrective actions that must be taken. It details the resources required, milestones, and scheduled completion dates. Detailed guidance on the POA&M process is found in Attachment H to this Handbook, *Plan of Action and Milestones (POA&M) Process Guide*.

When reviewing the authorization package, the AO may stipulate that certain POA&M activities be completed within a specific timeframe, or that additional compensating controls be implemented as a condition for authorization.

3.9.11 Authorization to Operate Letter

ATO or Denial to Operate letters are generated based on the appropriate AO’s decision after reviewing the authorization package. The package must include the following documents:

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

For operational systems, the AO makes a risk-based decision either to grant full ATO or deny authorization to operate. Authorizations to operate systems may be granted for a maximum of

three (3) years. Should Components require a system to operate in a production environment for six (6) months or less an ATO authorization period waiver from the DHS CISO is required.

The AO may grant an IATO for development, testing, or prototype systems. An IATO provides a limited authorization to operate the system under specified terms and conditions and acknowledges greater risk to the organization's operations and assets. A system undergoing development testing or a prototype system is *not* considered authorized during the IATO period.

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

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

3.9.12 Annual Self-Assessments

Annual assessments are performed during the Continuous Monitoring Phase of the authorization. They provide ongoing oversight and monitoring of the system's security controls and serve to inform the authorizing official whenever changes occur that may impact the security of the system. During this phase, the system's status is monitored to ensure that residual risk is kept within the acceptable level, and that any significant changes to the system configuration or operational or threat environment are identified. Components must re-authorize their systems every three (3) years or whenever a major change occurs.

The automated reporting tool, TAF addresses the annual self-assessments.

3.10 Information Security Review and Assistance

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

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

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

Information Security Review and Assistance Responsibilities
<p>DHS CIO</p> <p>Designates a full-time CISO</p> <p>Prepares the annual Congressional information security compliance report as required by FISMA</p> <p>DHS CISO</p> <p>Coordinates and prepares for the annual DHS Inspector General review of the Information Security Program</p> <p>Reviews and approves all DHS information security policies</p> <p>Establishes and implements an Information Security Review and Assistance Program</p> <p>Prepares and distributes a review and assistance handbook based on applicable NIST guidance</p> <p>DHS Compliance and Oversight Program Director</p>

Information Security Review and Assistance Responsibilities

Develops and implements a compliance review and assistance program

Component CISOs/ISSMs

Implement an Information Security Review and Assistance Program at the Component level

Schedule information security review and assistance visits and ensure that these visits are completed

Provide trained personnel to participate in review and assistance visits

Coordinate with ISSOs and provide guidance and oversight in identifying and documenting deficiencies and prioritizing them based on missions, risk, and funding

Review and monitor POA&Ms

Ensure that POA&M updates to the TAF database are timely (i.e., by March 10, June 10, September 15, and December 10 annually)

Coordinate issues with the Compliance and Oversight Program Director

Generate candidate information security policies, as the need arises, for CISO review and approval

Review NIST and other directives for applicability to the DHS Information Security Program

ISSOs

Prepare security self-assessment documentation as directed by the Component CISO/ISSM

Identify personnel qualified to participate in review and assistance visits

System Owners

Ensure that ISSOs have access to resources adequate for conducting self-assessments and review and assistance visits

Implement corrective actions for deficiencies found during self-assessments

Site Managers

Ensure that adequate personnel resources are available to participate in site assistance visits

3.10.1 Review and Assistance Management and Oversight

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

3.10.2 Information Security Assistance

Components shall provide on-site assistance to their organizations to the maximum extent practicable, in accordance with the Information Security Review and Assistance Program. Component CISOs/ISSMs shall coordinate with ISSOs and provide guidance and oversight in identifying deficiencies and prioritizing them based on missions, risk, and funding. The size and

geographic dispersion of DHS offices and organizations require close coordination and collaborative planning between the DHS CISO, Component CISOs/ISSMs, and ISSOs. Active support by site personnel and system development teams is imperative for the success of the assistance program.

3.10.3 Information Security Reviews

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

3.11 Security Working Groups and Forums

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

3.11.1 CISO Council

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

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

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

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

3.11.2 DHS Information Security Training Working Group

The DHS Information Security Training Working Group is established to promote collaboration on information security training efforts throughout the Department and to share information on

Component-developed training activities, methods, and tools, thereby reducing costs and avoiding duplication of effort. The Information Security Training Working Group is chaired by the DHS Program Director for Information Security Training.

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

3.11.3 DHS Security Policy Working Group

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

Policy ID	DHS Policy Statements	Relevant Controls
3.11.3.a	Each Component CISO shall appoint a representative to the DHS Security Policy Working Group.	---
3.11.3.b	The DHS Security Policy Working Group chair shall ensure that a report on representative attendance is made available to Component and Department CISOs.	---

3.12 Information Security Policy Violation and Disciplinary Action

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

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

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

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

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

3.13 Required Reporting

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

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

Components shall use TAF when reporting Information Security Program status.

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

Policy ID	DHS Policy Statements	Relevant Controls
	report generation.	

FISMA reporting responsibilities are provided in the following table.

FISMA Reporting Responsibilities
<p>Component CISO/ISSM/ISSO</p> <p>Ensure that the TAF automated tool is used for required reporting</p> <p>Ensure that Security Authorization Process artifacts (e.g., Privacy Impact Assessment, Security Plan, Security Test & Evaluation Report, Contingency Plan Test Results, Risk Assessment, ATO letter) are uploaded into TAF</p>

3.14 Privacy and Data Security

The DHS Privacy Office is responsible for privacy compliance across the Department, including assuring that technologies used by the Department sustain and do not erode privacy protections relating to the use of personal and Departmental information. The DHS Chief Privacy Officer has exclusive jurisdiction over the development of policy relating to Personally Identifiable Information (PII). Questions concerning privacy-related policy should be directed to the Component Privacy Office or Privacy Point of Contact (PPOC). If the Component does not have a Privacy Office or PPOC, then please contact the DHS Privacy Office (privacy@dhs.gov; 703-235-0780) or refer to the DHS Chief Privacy Officer Web page for additional information.

3.14.1 Personally Identifiable Information

Various regulations place restrictions on the Government's collection, use, maintenance, and release of information about individuals. Regulations require agencies to protect PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether or not the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or Department employee or contractor.

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

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

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

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

- A PTA provides a high level description of an information system including the information it contains and how it is used. The PTA is used to determine and document whether or not a PIA and/or SORN are required.
- A Privacy Impact Assessment (PIA) is a publicly released assessment of the privacy impact of an information system and includes an analysis of the PII that is collected, stored, and shared.
- A System of Records Notice (SORN) describes the categories of records within a system of records and describes the routine uses of the data and how individuals can gain access to records and correct errors.

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

3.14.2 Privacy Threshold Analyses

The PTA provides a high-level description of the system, including the information it contains and how it is used. PTAs are required whenever a new information system is being developed or an existing system is significantly modified. System Owners and Program Managers are responsible for writing the PTA as part of the SELC process. The Component Privacy Officer or PPOC reviews the PTA and forwards it to the DHS Privacy Office, who determines whether a PIA and/or SORN are required. PTA artifacts expire after three (3) years. DHS MD 0470.2 defines the PTA requirements.

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

PTA responsibilities are provided in the following table.

Privacy Threshold Analyses Responsibilities
<p>DHS Chief Privacy Officer</p> <ul style="list-style-type: none"> Reviews and approves the PTA Determines whether a system is a Privacy Sensitive System Determines whether a PIA and/or SORN are required Uploads validated PTAs to TAF <p>System Owner</p> <ul style="list-style-type: none"> Submits the PTA to the Component Privacy Officer or PPOC and provide any additional information required by the DHS Chief Privacy Officer to assist in the PTA process <p>Component Privacy Officer or PPOC</p> <ul style="list-style-type: none"> Reviews and submits the PTA for approval and provide any additional information required by the DHS Chief Privacy Officer to assist in the PTA process.

3.14.3 Privacy Impact Assessments

A PIA is a publicly released assessment of the privacy impact of an information system and includes an analysis of the PII that is collected, stored, and shared. PIAs are required (as determined by the PTA) whenever a new information system is being developed or an existing system is significantly modified. PIAs are the responsibility of the System Owner and the Program Manager as part of the SELC process. OMB Memorandum M-03-22, DHS MD 0470.1, and the *Official DHS Privacy Impact Assessment Guidance* discuss the requirements for conducting PIAs at DHS.

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

PIA responsibilities are provided in the following table.

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

3.14.4 System of Record Notices

The Privacy Act of 1974 requires a SORN when PII is maintained by a Federal agency in a system of records and the PII is retrieved by a personal identifier. A system of records is “a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual”⁷. The SORN describes the categories of records and individuals in the system of record; the routine uses of the data; how individuals can gain access to records pertaining to them and correct errors. The term “system of records” is not synonymous with “information system” and can include paper as well as electronic records. SORNs can be written to cover the records in a single group of records or a single information system or they can be written to cover multiple groups of records or multiple information systems.

Information systems that are considered a system of record may not be designated operational until a SORN has been published in the *Federal Register* for thirty days. OMB has issued the benchmark references for development of SORNs: *Privacy Act Implementation, Guidelines and Responsibilities*, July 9, 1975; *Circular A-130*, including Appendix I; DHS MD 0470.2, “Privacy Act Compliance;” October 6, 2005; and *Official DHS Guidance on System of Records and System of Records Notices*.

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

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

3.14.5 Protecting Privacy Sensitive Systems

OMB M-06-16, *Protection of Sensitive Agency Information* requires that agencies protect PII that is physically removed from Department locations or is accessed remotely. Physical removal includes both removable media and media in mobile devices (e.g., laptop hard drives). Please

⁷ 5 U.S.C. §552a(a)(5) *Italics added.*

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

- [“Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security”](#):
- This Handbook’s Attachment S, “Compliance Framework for Privacy Sensitive Systems”
- This Handbook’s Attachment S1: “Policy and Procedures for Managing Computer-Readable Extracts Containing Sensitive PII.”

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

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

Policy ID	DHS Policy Statements	Relevant Controls
	Component Privacy Officer or PPOC.	

3.14.6 Privacy Incident Reporting

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

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

Incident reporting responsibilities are provided in the following table.

Privacy Incident Reporting Responsibilities

DHS Personnel

Provides notification of incident to Program Manager (PM)

Attend annual Privacy Awareness Training and Education.

Recognize Privacy Incidents.

Inform the PM of the detection or discovery of suspected or confirmed incidents involving PII; or if PM is unavailable, contact the Help Desk for the Component.

Program Manager

Prepares preliminary privacy incident report and passes report to the Component CISO/ISSM or Component SOC

Ensure compliance with federal laws and Departmental privacy policy concerning the operation and maintenance of information systems and programs.

Recognize Privacy Incidents.

Understand the Component's Privacy Incident reporting process and procedures Receive initial reports from DHS personnel regarding the detection of possible Privacy Incidents.

Consult with the Component Privacy Officer/PPOC for guidance concerning Privacy Incident handling and other privacy issues affecting information systems.

Determine whether a suspected or confirmed incident involving PII has occurred.

Provide a brief preliminary written report to the Component IT security entity (ISSM or Component SOC, or if the Component IT security entity is not available, contact the DHS SOC directly.

Assist the Component Privacy Officer/PPOC and the Component IT Security Entity with the development of facts for the Privacy Incident Report.

Provide advice, expertise, and assistance to the Privacy Incident Response Team (PIRT) as needed.

Assist with the investigation and mitigation of a Privacy Incident.

Component CISO/ISSM/Component SOC

Evaluates Privacy Incident; Prepares and Submits Incident Report in SOC Online Incident Handling System

DHS SOC

Notifies Chief Privacy Officer, DHS Deputy Secretary, DHS CPO, DHS CIO, DHS Deputy CIO, DHS OGC-GLD CISO, CIO and Dep. CIO; Processes and Transmits Privacy Incident Report to US-CERT

3.14.7 E-Authentication

Identity verification or authentication (e-authentication) is needed to ensure that online Government services are secure and that individual privacy is protected. Each DHS system must be evaluated to determine whether e-authentication requirements apply. Only federated identity providers approved through the Federal CIO Council's Identity, Credentialing, and Access

Management’s (ICAM) Trust Framework Provider Adoption Process (TFPAP) should be used. Components should see www.IDmanagement.gov for details regarding the Federal Identity, Credentialing, and Access Management (FICAM) initiative.

E-authentication guidance is provided in the following:

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

Policy ID	DHS Policy Statements	Relevant Controls
3.14.7.a	For systems that allow online transactions, Components shall determine whether e-authentication requirements apply.	IA-2
3.14.7.b	Components shall determine the appropriate assurance level for e-authentication by following the steps described in OMB Memorandum M-04-04, “E-Authentication Guidance for Federal Agencies.”	IA-2
3.14.7.c	Components shall implement the technical requirements described in NIST SP 800-63, Rev 1, Draft 3 “Electronic Authentication Guideline,” at the appropriate assurance level for those systems with e-authentication requirements.	IA-2
3.14.7.d	Components shall ensure that each SP reflects the e-authentication status of the respective system.	IA-2, PL-2
3.14.7.e	Programs considering the use of e-authentication are required to consult their privacy officer to determine whether a change is significant enough to warrant a new or updated PTA, thus initiating the review of privacy risks and how they will be mitigated.	PL-5
3.14.7.f	Existing physical and logical access control systems shall be upgraded to use PIV credentials, in accordance with NIST and DHS guidelines.	
3.14.7.g	All new systems under development shall be enabled to use PIV credentials, in accordance with NIST and DHS guidelines, prior to being made operational.	
3.14.7.h	All new DHS information systems or those undergoing major upgrades shall use or support DHS PIV credentials.	---

3.15 DHS CFO Designated Systems

DHS CFO Designated Systems are systems that require additional management accountability to ensure effective internal control exists over financial reporting. The DHS CFO publishes the approved list of CFO Designated Systems annually. This section provides additional requirements for these systems based on Appendix A to OMB Circular A-123, “Management’s Responsibility for Internal Control.” The requirements contained in OMB Circular A-123 have

been mapped to the NIST SP 800-53 controls and documented in Attachment R to this Handbook, “Compliance Framework for CFO-Designated Financial Systems.” These requirements are in addition to both the other security requirements established in this Policy Directive and other CFO-developed financial system Line of Business requirements.

Wherever there is a conflict between this section and other sections of this Policy Directive regarding requirements for CFO Designated Systems, this section shall take precedence.

These additional requirements provide a strengthened assessment process and form the basis for management’s assurance of internal control over financial reporting. The strengthened process requires management to document the design and test the operating effectiveness of controls for CFO Designated Systems. The system owner is responsible for ensuring that all requirements, including security requirements, are implemented on DHS systems. Component CISOs/ISSMs must coordinate with their CFO organization to ensure that these requirements are implemented.

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

Policy ID	DHS Policy Statements	Relevant Controls
3.15.i	The SP shall be updated for CFO Designated Systems at least annually. Key controls prescribed in Attachment R, <i>Compliance Framework for CFO Designated Systems</i> shall be identified in the SP.	PL-2
3.15.j	Component CISOs/ISSMs must request a waiver or exception from the DHS CISO if a key control weakness is identified for a CFO Designated System and not remediated within twelve (12) months.	CA-5, CA-7
3.15.k	Component CFOs shall ensure that a fulltime dedicated ISSO is assigned to each CFO Designated System. CFO Designated System ISSOs may be assigned to more than one CFO Designated System.	---
3.15.l	CFO Designated System ATOs shall be rescinded if Components fail to comply with testing and reporting requirements established within this policy.	CA-1, CA-6
3.15.m	Component CFOs shall work with their Component CISOs/ISSMs to approve any major system changes to CFO Designated Systems identified in the DHS inventory.	CA-1, CM-8

OMB A-123, Appendix A, “Implementation Plans,” defines two types of system controls: Information Technology General Controls (ITGC) and Application Controls. This Handbook accounts for the ITGCs, which address structure, policies, and procedures related to an ‘entity’s’ overall computer operations. ITGCs are not tied to any one business process, but may be related to a number of applications, associated technical infrastructure elements, and information systems management organizations that support Line of Business processes.

The *Federal Information System Controls Audit Manual (FISCAM)*, which provides guidance on how to incorporate robust and secure financial auditing controls, is used to assess ITGCs. Application controls as defined by OMB Circular A-123 provide controls over input, processing, and output of data associated with individual applications, and are not addressed in this Handbook.

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

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

Artifact	Required Action	Frequency	Completion Deadline	Reporting Requirements
----------	-----------------	-----------	---------------------	------------------------

Artifact	Required Action	Frequency	Completion Deadline	Reporting Requirements
Risk Assessment (RA)	A complete RA shall be conducted	Annual	As determined by the Component CISO/ISSM	Report no later than (NLT) Sep 30 of each year
Security Plan (SP)	The SP shall be evaluated and updated	Annual	During first quarter of each FY	Report NLT Sep 30 of each year
Key Security Controls Security Assessment Results	Key security controls shall be evaluated and updated	Annual	During first quarter of each FY	Report completion NLT Dec 31 of each year
Disaster Recovery (DR) Plan Results	The DR plan shall be exercised	Annual	First quarter of each FY	Report completion NLT Dec 31 of each year
Vulnerability Assessment (VA)	A complete VA shall be conducted	Semi-Annual	One assessment completed during the first quarter of each FY; Second assessment completed during the third quarter.	Report completion of one assessment NLT Dec 31; report completion of second assessment NLT Jun 30
Critical Patch Installation	Installation of critical patches shall be verified	Semi-Annual	As determined by the Component CISO/ISSM	Report NLT Sep 30 of each year

Table 1 – Documentation and Testing Artifacts

3.16 Social Media

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

Policy ID	DHS Policy Statements	Relevant Controls
3.16.a	Only OPA-designated content managers (Department level and Component level) may post content, and only those individuals designated by OPA for this purpose shall be granted access on a continuing basis.	SA-6
3.16.b	Posted content shall be in keeping with the Department's Terms of Service (TOS) and guidelines for a given social media host (e.g., YouTube, Twitter). This condition is also met if the Department endorses another appropriate Federal agency's guidance or TOS (e.g., GSA, OPM). Under no circumstances shall sensitive information be posted to social media sites.	---
3.16.c	Content shall not be posted to any social media site for which the Department has not approved and published <i>both</i> final posting guidelines <i>and</i> TOS.	SA-6
3.16.d	Content managers shall review and understand the appropriate Department-level TOS for the appropriate social media host.	---
3.16.e	Content managers shall make a risk decision prior to posting any information and shall recognize that social medial hosts are not DHS information systems and therefore subject only to the DHS TOS and not to DHS policy. Once released, information is no longer under DHS control.	---

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

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

3.17 Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)⁸ addresses the privacy of individuals' health information by establishing a Federal privacy standard for health information and how it can be used and disclosed.

⁸ Public Law 104-191

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

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

Policy ID	DHS Policy Statements	Relevant Controls
3.17.a	Components whose systems collect, process, or store Protected Health Information (PHI) shall ensure that the stored information is appropriately protected in compliance with HIPAA and that access or disclosure is limited to the minimum required.	---
3.17.b	Affected Components shall work with the DHS Privacy Office, Component Privacy Office, or PPOC to ensure that privacy and disclosure policies comply with HIPAA requirements.	---
3.17.c	Affected Components shall ensure that employees with access to DHS systems that collect, process, or store PHI are trained in HIPAA requirements.	---
3.17.d	Affected Components shall establish administrative processes for responding to complaints; requesting corrections to health information; and tracking of PHI disclosures.	---
3.17.e	When collecting PHI, Components shall issue a privacy notice to individuals concerning the use and disclosure of their PHI.	---

3.18 Cloud Services

Cloud computing offers a unique opportunity for DHS to take advantage of proven new information technologies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services provided to its employees. Consistent with the President's International Strategy for Cyberspace and with the Cloud First policy, the adoption and use by DHS of information systems operated by cloud service providers (cloud services) depends on security, interoperability, portability, reliability, and resiliency.

In accordance with the OMB Memorandum *Security Authorization of Information Systems in Cloud Computing Environments*, the Federal Risk and Authorization Management Program (FedRAMP) will provide a cost-effective, risk-based approach for the adoption and use of cloud services by making available to Executive departments and agencies:

- Standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels

- A conformity assessment program capable of producing consistent independent, third-party assessments of security controls implemented by CSPs
- Authorization packages of cloud services reviewed by a Joint Authorization Board (JAB) consisting of security experts from the DHS, DOD, and GSA

Standardized contract language to help Executive departments and agencies integrate FedRAMP requirements and best practices into acquisition

- A repository of authorization packages for cloud services that can be leveraged government-wide

FedRAMP will reduce duplication of effort, inconsistencies, and cost inefficiencies associated with the current security authorization process. FedRAMP establishes a public-private partnership to promote innovation and the advancement of more secure information technologies. By using an agile and flexible framework, FedRAMP will enable the Government to accelerate the adoption of cloud computing by creating transparent standards and processes for security authorizations and by allowing agencies to benefit from the leverage of Government-wide security authorizations.

Policy ID	DHS Policy Statements	Relevant Controls
3.18.a	Components shall use FedRAMP when conducting risk assessments and security authorizations and granting ATOs for use of cloud services.	---
3.18.b	All DHS cloud services shall be assessed by a Third Party Assessment Organization (3PAO) that has been accredited using a process that follows the conformity assessment approach outlined in ISO/IEC 17020, <i>General Criteria for the operation of various types of bodies performing inspection (1998)</i> .	---

4.0 OPERATIONAL CONTROLS

4.1 Personnel

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

4.1.1 Personnel Screening and Position Categorization

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

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

Sensitivity levels for all Government positions involving the use, development, operation, or maintenance of information systems shall be designated, and risk levels for each contractor position shall be determined.

Policy ID	DHS Policy Statements	Relevant Controls
4.1.1.a	Components shall designate the position sensitivity level for all Government and contractor positions that use, develop, operate, or maintain information systems and shall determine risk levels for each contractor position. Position sensitivity levels shall be reviewed annually and revised as appropriate.	PS-2, PS-3, PS-7
4.1.1.b	Components shall ensure that the incumbents of these positions have favorably adjudicated background investigations commensurate with the defined position sensitivity levels.	PS-2, PS-3, PS-7
4.1.1.c	Components shall ensure that no Federal employee is granted access to any DHS system without having a favorably adjudicated Moderate Risk Background Investigation (MBI) as defined in DHS Instruction 121-01-007, <i>Personnel Suitability and Security Program</i> , Chapter 2, Federal Employee/Applicant Suitability Requirements. In cases where non-DHS Federal employees have been investigated by another Federal agency, DHS Component personnel security organizations may, whenever practicable, use these investigations to reduce investigation requests, associated costs, and unnecessary delays (Chapter 2, paragraph G). Active duty United States Coast Guard (USCG) and other personnel subject to the Uniform Code of Military	PS-3

Policy ID	DHS Policy Statements	Relevant Controls
	Justice (UCMJ) shall be exempt from this requirement.	
4.1.1.d	Components shall ensure that no contractor personnel are granted access to DHS systems without having a favorably adjudicated Background Investigation (BI) as defined in <u>Department of Homeland Security Acquisition Regulation (HSAR)</u> and the DHS Instruction 121-01-007, <i>Personnel Suitability and Security Program</i> , Chapter 3, Excepted Service Federal Employee and Contractor Employee Fitness Requirements. In cases where contractor personnel have been investigated by another Federal agency, DHS Component personnel security organizations may, whenever practicable, use these investigations to reduce investigation requests, associated costs, and unnecessary delays (Chapter 3, paragraph G).	PS-3
4.1.1.e	Components shall ensure that only U.S. Citizens are granted access to DHS systems and networks. Exceptions to the U.S. Citizenship requirement may be granted by the Component Head or designee with the concurrence of the Office of Security and the DHS Chief Information Officer (CIO), in accordance with Section 1.5.4, of this policy, "Requests for Exception to U.S. Citizenship Requirement."	PS-3

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

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

4.1.1.1 Background Investigations for Government Employees

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

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

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

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

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

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

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

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

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

4.1.1.2 Background Investigations for Contractor Personnel

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

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

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

** Eligible for access only to the moderate risk level

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

4.1.2 Rules of Behavior

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

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

access to any system; and must state the consequences of inconsistent behavior or noncompliance.

ROB for individual systems may be inherited from organizational rules or site Rules of Behavior (e.g. an individual local area network (LAN) GSS Rules of Behavior may be automatically included as part of an organization-wide GSS ROB to which all employees and staff are held accountable).

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

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

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

Policy ID	DHS Policy Statements	Relevant Controls
4.1.2.a	Components shall ensure that rules of behavior contain acknowledgement that the user has no expectation of privacy (a “Consent to Monitor” provision) and that disciplinary actions may result from violations.	PL-4
4.1.2.b	Components shall ensure that DHS users are trained regarding rules of behavior and that each user signs a copy prior to being granted user accounts or access to information systems or data.	AT-1, AT-2, PL-4

Rules of Behavior responsibilities are provided in the following table.

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

Rules of Behavior Responsibilities
Adhere to all Rules of Behavior for the systems to which they have been granted access

4.1.3 Access to Sensitive Information

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

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

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

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

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

4.1.4 Separation of Duties

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

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

Assignment and segregation of system responsibilities must be clearly defined and documented for all DHS systems. Segregation of responsibilities, in addition to appropriate access controls, is

intended to ensure that no individual has all necessary authority or information access needed to engage in fraudulent activity without collusion. It is essential that thorough and specific job descriptions be documented for every individual working with DHS systems and sensitive information.

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

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

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

Policy ID	DHS Policy Statements	Relevant Controls
4.1.4.a	Components shall divide and separate duties and responsibilities of critical information system functions among different individuals to minimize the possibility that any one individual would have the necessary authority or system access to be able to engage in fraudulent or criminal activity.	AC-2, AC-5
4.1.4.b	All individuals requiring administrator privileges shall be reviewed and approved by the appropriate AO. The AO may delegate this duty to the appropriate system owner or Program Manager.	AC-2
4.1.4.c	Individuals requiring administrator privileges shall be assigned administrator accounts separate from their normal user accounts.	AC-6
4.1.4.d	Administrator accounts shall be used only for performing required administrator duties. Individuals shall use their regular user accounts to perform all other functions not directly tied to administrator duties (checking email, accessing the Internet).	AC-6

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

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

4.1.5 Information Security Awareness, Training, and Education

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

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

Information security training must be addressed in the Security Plan for each system. Additionally, Component CISOs/ISSMs⁹ shall prepare and submit an annual training plan for information security awareness, training, and education to the DHS Information Systems Security Training Program Director. Plans shall follow the guidance in the DHS Information Technology Security Awareness, Training and Education Plan template, issued by the DHS Information Systems Security Training Office.

OPM requires Federal agencies to provide training to the following groups within 60 days of their appointment:¹⁰

- Executives
- Program and functional managers
- Information resources management

⁹ CISO: Chief Information Security Office; ISSM; Information Systems Security Manager

¹⁰ In 5 CFR Part 930,

- Security audit personnel
- Information system managers and operations personnel

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

4.1.5.1 Initial Awareness

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

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

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

4.1.5.2 Refresher Awareness

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

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

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

4.1.5.3 Ongoing Awareness Activities

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

4.1.5.4 Role-Based Training

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

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

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

Policy ID	DHS Policy Statements	Relevant Controls
	role-based training programs annually.	
4.1.5.k	Components shall submit a roster the during the first month and during the seventh month of each fiscal year identifying all significant information security personnel, including full name, security role, employment status (federal employee, military, contractor), and work location (state). At a minimum, the roster will include all standard information security roles: Chief Information Officer, Chief Information Security Officer, Authorizing Official, Program Manager, System Owner, Information System Security Officer, Security Operations Center Manager, System Administrator (Windows-based), and Contracting Officer/Contracting Officer Representative.	AT-1

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

Information Security Awareness, Training, and Education Responsibilities
<p>Component CISOs/ISSMs</p> <ul style="list-style-type: none"> Establish overall policy for information security awareness, training, and education Provide guidance on preparing and attending security awareness and training sessions Submit a training plan outlining plans for Information Security Awareness, Training, and Education for the year to the DHS Information Security Training Program Director Analyze security awareness and training statistics submitted by the ISSOs and COTRs and submit a summary of these statistics to the DHS Information Security Training Program Director on a quarterly basis <p>ISSOs</p> <ul style="list-style-type: none"> Ensure that all new employees, including contractors, complete an initial security awareness course as part of their orientation Unless a Component CISO/ISSM waiver is issued, disable all accounts and access privileges, including access to email, of those DHS users who failed to complete the annual security refresher course Ensure that all users read and sign the appropriate Rules of Behavior prior to being granted access to systems and applications Implement annual awareness refresher training for employees and support contractors involved in the management, use, or operation of DHS systems Maintain a record of security awareness and training that includes the name and position of the person trained, the type of training, the date of the training, and the cost of the training Submit statistics on initial and refresher security awareness and training to the Component CISO/ISSM, on a quarterly basis Implement additional training for personnel when there is a significant change in the system security

Information Security Awareness, Training, and Education Responsibilities

environment or in procedures, or when an employee enters a new position involving the handling of sensitive information

COTRs

Ensure that contractors have their personnel complete an initial security awareness course as part of their orientation

Ensure that contractors have their personnel complete an annual refresher security awareness course

Ensure that contractors have their personnel sign the appropriate Rules of Behavior for use of systems and applications prior to receiving access

Ensure that contractors provide additional security awareness training to their personnel whenever there is a significant change in the system security environment or in procedures, or when contractor personnel enter a new position

Ensure that contractors maintain a training record for their personnel who have completed initial and refresher security awareness training; the record shall include the name of the person trained, the type and date of the training, and training cost

Ensure that contractor security awareness and training statistics are provided to the Component CISO/ISSM on a quarterly basis

4.1.6 Separation from Duty

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

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

In all cases, Components shall adhere to the following:

- Revoke all authorizations
- Retrieve hard and soft copy sensitive information
- Retrieve all keys, badges, and other access devices
- Change locks
- Retrieve Government-owned equipment (laptops, cell phones, portable electronic devices (PED), secure ID tokens, etc.)
- Conduct exit interview

Policy ID	DHS Policy Statements	Relevant Controls
4.1.6.a	Components shall implement procedures to ensure that system access is revoked for DHS employees, contractors, or others working on behalf of DHS who leave the Component, are reassigned to other duties, or no longer require access.	AC-2
4.1.6.b	Components shall establish procedures to ensure that all DHS property and assets related to information systems are recovered from the departing individual and that sensitive information stored on any media is transferred to an authorized individual.	PS-4
4.1.6.c	Accounts for personnel on extended absences shall be temporarily suspended.	AC-2
4.1.6.d	System Owners shall review information system accounts supporting their programs at least annually.	AC-2

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

Separation from Duty Responsibilities
<p>System Owners/Senior Site Managers</p> <p>Implement procedures to ensure appropriate system access privileges are revoked for employees or contractors who either leave the Component or are reassigned to other duties</p> <p>Supervisors</p> <p>Notify system administrators in writing when employees or contractors no longer require access to DHS systems</p> <p>Retrieve all sensitive data from departing employees and contractors</p> <p>Network/System Administrators</p> <p>Disable or delete user accounts when notified that an individual's access to DHS systems is reassigned or terminated</p> <p>Site Security Officers</p> <p>Change combinations to all locks and safes whenever an employee or contractor with access has been reassigned or terminated</p> <p>Collect all keys, badges, and other devices used to gain access to premises, information, or equipment from employees and contractors who have been terminated or reassigned</p> <p>Employees, Contractors, or Others Working on Behalf of DHS</p> <p>Turn in laptops, cell phones, PEDs, secure ID tokens, and other Government-owned devices to the local property administrator in accordance with local procedures when reassigned or terminated</p>

4.2 Physical Security

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

4.2.1 General Physical Access

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

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

General physical access responsibilities are provided in the following table.

General Physical Access Responsibilities
Facility Managers

General Physical Access Responsibilities

Ensure that physical controls are in place

Ensure that environmental controls are in place

Ensure that physical and environmental controls are in working order at all times

Ensure that access control logs are maintained and reviewed for the facility and all computer rooms

Site Security Officers/ISSOs

Provide specific security briefings to DHS employees and contractors

Assess the adequacy of physical security controls as part of the risk management cycle

Change combinations to locks on security containers housing sensitive information, funds, and other valuables that must be safeguarded

Conduct periodic inspections of offices and areas under their jurisdiction, during or after working hours, to ensure that sensitive and proprietary materials are being adequately safeguarded

Ensure that security violations are appropriately reported and investigated, in accordance with DHS requirements

Provide oversight of the issuing and return of service badges, credentials, and identification documents, and ensure proper reporting of their loss or theft

Apply security disciplines to the contractor environment

Ensure that Government-owned and controlled property, funds, and valuables are properly safeguarded and accounted for

Ensure the physical security of information systems within their jurisdiction

Ensure that physical and environmental security controls are addressed in the Security Plan

Address physical security as an integral part of the risk management process

Ensure that physical security risks are reviewed and evaluated throughout the Systems Engineering Life Cycle (SELC)

Users

Adhere to established security policies

Display building passes or other ID when required

Challenge individuals who are not in compliance with established requirements

Ensure that uncleared visitors are escorted at all times

4.2.1.1 Physical Controls

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

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

- Controlled access to building (i.e., physical building access, guards)
- Controlled access to computer room(s)
- Locks
- Key control procedures
- Keypads and cipher locks
- ID badges (worn above the waist area)
- Visitor logs
- Biometric devices
- Access control logs (to the building)
- Access control logs (to the computer rooms and facility)
- Motion detectors
- Intrusion detection devices
- Property passes
- Additional controls

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

4.2.1.2 Building Passes

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

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

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

4.2.1.3 Property Removal

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

4.2.1.4 Loss or Theft of Property

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

4.2.1.5 Environmental Controls

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

- Fire protection, detection, and suppression
- Water damage risk reduction, detection, and corrective measures, and devices for water hazard prevention
- Electronic power supply protection, to include uninterruptible power supplies for multi-use systems and surge protectors for stand-alone systems
- Temperature and humidity recording, monitoring, and alert systems
- Housekeeping protection from dirt and dust
- Combustible cleaning supplies protection (not to be kept in computer areas)
- Appropriate personnel safety features (evacuation routes specified)
- Emergency exit provisions, such as equipping emergency and exit-only doors with hardware that permits immediate egress in the event of an emergency

4.2.1.6 Fire Protection

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

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

4.2.1.7 Electronic Power Supply Protection

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

4.2.1.8 Temperature and Humidity Control

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

- Temperatures in computer storage areas should be held between 60 and 70 degrees Fahrenheit. Most systems will continue to function when temperatures go beyond this range,

but the associated risk to data is increased. (Check individual system documentation for the proper levels.)

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

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

4.2.1.9 Housekeeping Considerations

Housekeeping is another important area to monitor.

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

4.2.1.10 Personnel Safety Features

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

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

4.2.1.11 Emergency Exits

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

4.2.2 Sensitive Facility

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

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

Policy ID	DHS Policy Statements	Relevant Controls
	reflected in this and other relevant documents.	

4.3 Media Controls

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

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

4.3.1 Media Protection

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

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

Policy ID	DHS Policy Statements	Relevant Controls
4.3.1.a	Components shall ensure that all media containing sensitive information, including hard copy media, backup media, and removable media such as USB drives, are stored when not in use in a secure location (e.g., a locked office, room, desk, bookcase, file cabinet, locked tape device, or in other storage that prohibits access by unauthorized persons).	MP-2, MP-4, PE-1
4.3.1.b	Components shall ensure that all offsite backup media are protected as per guidance in this section.	CP-6
4.3.1.c	DHS personnel, contractors, and others working on behalf of DHS are prohibited from using any non-Government-issued removable media (USB drives, in particular) and from connecting them to DHS equipment or	MP-2

Policy ID	DHS Policy Statements	Relevant Controls
	networks or using them to store DHS sensitive information.	
4.3.1.d	Systems requiring encryption shall comply with Section 5.5.1, Encryption, of this Policy Directive. DHS-owned USB drives shall use encryption.	IA-7, SC-13
4.3.1.e	DHS-owned removable media shall not be connected to any non-DHS information system unless the AO has determined that the risk is acceptable based on compensating controls and published acceptable use guidance that has been approved by the respective CISO or Information Systems Security Manager (ISSM). (The respective CISO is the CISO with that system in his or her inventory.)	AC-20, MP-2, PM-9
4.3.1.f	Components shall follow established procedures to ensure that paper and electronic outputs from systems containing sensitive information are protected.	MP-1
4.3.1.g	Users shall ensure proper protection of printed output. Printing of sensitive documents shall occur only when a trusted person is attending the printer.	SI-12
4.3.1.h	Components shall follow the procedures established by DHS MD 11042.1, “Safeguarding Sensitive But Unclassified (For Official Use Only) Information,” for the transportation or mailing of sensitive media.	MP-5

Media protection responsibilities are provided in the following table.

Media Protection Responsibilities
<p>DHS CISO Establishes and enforces DHS policy relating to labeling, storage, media reuse, and disposal of DHS equipment</p> <p>System Owners Ensure that any special storage requirements are communicated to the Project Manager and system administrators</p> <p>System/Network Administrators Ensure that sensitive information is stored in a locked container or in an area with adequate access controls to prevent unauthorized access, disclosure, damage, modification, or destruction Ensure that recipients of sensitive information have a valid “need to know” and proper authorization Ensure that copies of backups are stored at secure offsite locations</p> <p>Facility Managers Ensure that sensitive information is stored in a locked container or in an area with adequate access</p>

Media Protection Responsibilities

controls so as to prevent unauthorized access, disclosure, damage, modification, or destruction

Establish both onsite and offsite storage locations

Establish and maintain an inventory accounting system for all media entering or leaving a media storage area.

Ensure that inventory is verified at least semiannually

Ensure that backup storage facilities meet the minimum requirements enumerated in Section 4.11, Information and Data Backup

ISSOs

Ensure that media are stored in accordance with the requirements enumerated in this handbook

Ensure that storage requirements are addressed in the Security Plan and Rules of Behavior

4.3.2 Media Marking and Transport

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

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

The following definitions apply within this section:

- **Hardcopy Material** – Printed material, including reports, emails, briefings, manuals, guidance, letters, and memoranda
- **Label** – A piece of information that indicates the sensitivity level of an object and the information it contains. A label may be internal or external as follows:
 - **Internal Label** – A marking that reflects the sensitivity of the information within the confines of the medium
 - **External Label** – Has a visible marking on the outside of the medium, or a cover that reflects the sensitivity of the information contained
- **Storage Media** – Includes but is not limited to magnetic storage media such as hard disk drives and diskettes; optical storage media such as CDs and DVDs; solid-state storage media, including USB drives; and hardcopy materials, including reports, emails, briefings, manuals, guidance, letters, and memoranda.

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

Policy ID	DHS Policy Statements	Relevant Controls
4.3.2.a	Media determined by the information owner to contain sensitive information shall be appropriately marked in accordance with DHS MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information .	MP-3
4.3.2.b	Components shall control the transport of information system media containing sensitive data, outside of controlled areas and restrict the pickup, receipt, transfer, and delivery to authorized personnel.	MP-5

Media marking responsibilities are provided in the following table.

Media Marking Responsibilities
<p>DHS CISO Establishes and enforces policy relating to labeling, storage, reuse, and disposal of media containing sensitive information</p> <p>System Owners Ensure that mission security needs are communicated to Project Managers and system administrators</p> <p>Project Managers Implement electronic marking requirements and warning banners for automated systems</p> <p>System Administrators Implement electronic marking requirements and warning banners on their systems</p> <p>ISSOs Ensure that sensitive systems and information are appropriately identified and that sensitivity and criticality levels are established for each system Ensure that marking requirements are addressed in the SP and that areas of noncompliance are identified Ensure that automated system and site personnel understand and are adequately trained in the identification and marking of sensitive information Ensure that marking procedures and warning banners are reviewed with all personnel periodically, such as during annual Computer Security Awareness sessions Ensure that all users are aware of the value and sensitivity of information Ensure that users understand their responsibilities for safeguarding sensitive DHS information and know how to fulfill their responsibilities Ensure that procedures are in place to ensure that all personnel follow guidelines and procedures for marking media containing sensitive information</p>

4.3.3 Media Sanitization and Disposal

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

Policy ID	DHS Policy Statements	Relevant Controls
4.3.3.a	Components shall ensure that any information systems storage medium containing sensitive information is sanitized using approved sanitization methods before it is disposed of, reused, recycled, or returned to the owner or manufacturer.	MP-6
4.3.3.b	Components shall maintain records of the sanitization and disposition of information systems storage media.	MP-6
4.3.3.c	Components shall test degaussing equipment to verify that the equipment is functioning properly, at least once every 3 years or whenever an question as to the efficacy of the equipment exists.	MP-6

Media sanitization responsibilities are provided in the following table.

Media Sanitization Responsibilities
<p>Site Managers</p> <ul style="list-style-type: none"> Allocate resources to meet media sanitization requirements Enforce media sanitization requirements <p>Component CISOs/ISSMs</p> <ul style="list-style-type: none"> Develop and implement media sanitization procedures for storage media that are to be disposed of, recycled, reused, returned to the owner, or returned for repair or replacement <p>ISSOs</p> <ul style="list-style-type: none"> Ensure that media sanitization requirements are addressed in the SP and Security Operating Procedures Maintain records of the sanitization and disposition of sensitive storage media <p>System/Network Administrators</p> <ul style="list-style-type: none"> Ensure that storage media for disposal, recycling, or reuse are properly sanitized Ensure that leased storage media are properly sanitized before they are returned to the owner Ensure that defective or inoperable storage media are properly sanitized before they are returned to the vendor or manufacturer for repair or replacement Ensure that defective or inoperable storage media that cannot be sanitized are physically destroyed and disposed of

Media Sanitization Responsibilities
Periodically test degaussing equipment to ensure proper operation
Users
Ensure the safekeeping of sensitive storage media
Notify ISSO or Site Security Manager when media containing sensitive information are no longer required

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

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

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

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

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

- **Clearing** is removal of information stored on media in such a way that the information is irretrievable through means such as robust keyboard attacks or the use of data, disk, or file recovery techniques. For magnetic media such as hard drives and diskettes, simple deletion of files is not sufficient for clearing, as the deleted data can be retrieved by various recovery utilities. Overwriting the information with random data, however, will clear the media of information and will help ensure that the information is irretrievable except perhaps by advanced laboratory techniques. Overwriting cannot be used for magnetic media that are damaged or not writeable. In such cases, the media must be physically destroyed.

- **Purging** is removal of information stored on media in such a way that the information is irretrievable through any means, including advanced laboratory techniques. Executing the firmware Secure Erase command and degaussing are examples of acceptable methods for purging. Degaussers expose the medium to a strong magnetic field, which effectively erases the information (a degausser designed and approved for the type of medium being purged is required). Be aware that degaussing also destroys hard drives, as the firmware that manages the drive is also purged during the degaussing process. Degaussing is effective only on magnetic media such as hard drives, diskettes, and magnetic tapes. It is not effective on optical media such as CDs and DVDs.
- **Destruction** of media is the ultimate form of sanitization. Physical destruction can be accomplished through disintegration, incineration, pulverizing, shredding, and melting. Destruction of media should be conducted only by trained and authorized personnel. Safety, hazmat, and special disposition needs should be identified and addressed prior to conducting any media destruction.

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

Steps for sanitizing of media are as follows:

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

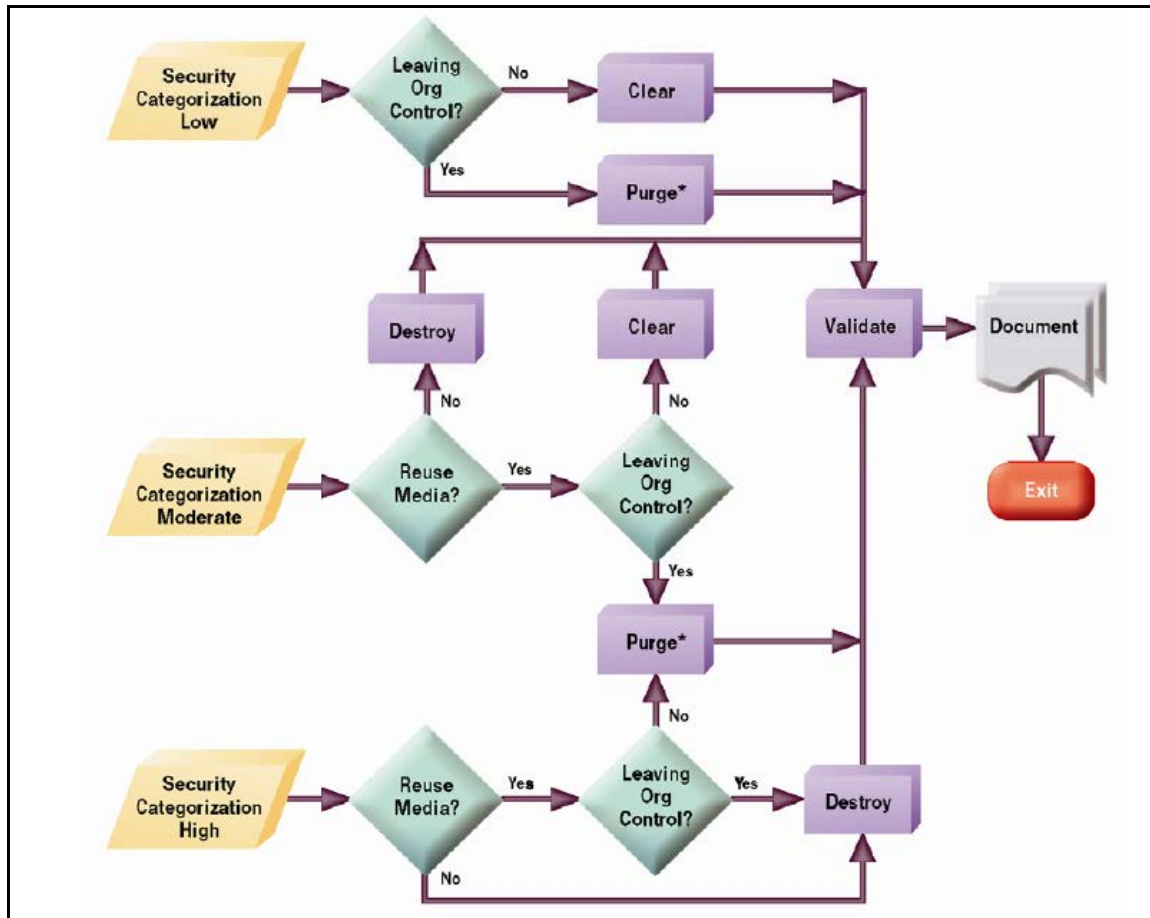


Figure 2 – Flowchart depicting the process for selecting media sanitization method, by categorization of impact for the confidentiality security objective.

(Adapted from NIST SP 800-88)

4.3.4 Production, Input/Output Controls

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

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

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

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

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

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

4.4 Voice Communications Security

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

4.4.1 Private Branch Exchange

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

Potential threats to a PBX include:

- Unauthorized access
- Traffic analysis

- Theft of service
- Disclosure of information
- Data modification
- Denial of service

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

- **External access/control** – PBXs typically require remote maintenance by vendors. Local administrators often have the manufacturer remotely install updates, which requires remote maintenance ports and access to the switch by a potentially large pool of outside parties.
- **Feature richness** – The wide variety of features available on PBXs, particularly administrative features and conference functions, allow for the possibility of unexpected attacks. An attacker may eavesdrop by using features in a manner not intended by its designers. Features may also interact in unpredictable ways, leading to system compromise even if each element of the system conforms to its security requirements and the system operation and administration are correct.

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

PBX security responsibilities are provided in the following table.

PBX Security Responsibilities
<p>Component CISOs/ISSMs</p> <p>Provide guidance concerning appropriate PBX-related security training to include:</p> <ul style="list-style-type: none"> – Types of information personnel should not release to callers – Security requirements for new PBX systems (e.g., disable test accounts, passwords, and shortcut keys) and for maintenance activities for distribution to vendors <p>Site Managers</p> <p>Ensure that employees and others with access to the facilities have agreed to and signed a PBX policy statement</p> <p>Ensure that PBX contracts and maintenance agreements include information on disputes, how they are settled, and the appeals process. Obtain approval from legal team before implementing</p> <p>Explicitly include the requirements for integrity, availability, and confidentiality protection in the</p>

PBX Security Responsibilities

PBX, and directly address liability in PBX contractual agreements

Develop specific guidelines on acceptable and unacceptable use of telecommunications within the organization, and specify how the PBX policy deals with actions not explicitly covered by the general information security policy

ISSOs

Address PBX issues in annual awareness sessions for all employees

Identify, in the policy statement, the personnel or position(s) responsible for telephone usage

Ensure that agreements with the local exchange carrier (LEC), the inter-exchange carrier (IXC), and the equipment vendors allow only authorized personnel to request service level changes, and to report errors

Verify all toll calls billed against PBX traffic reports

Ensure that internal PBX audits include verification that all records are in electronic form

Ensure that internal information systems auditors complete an audit of each PBX system at least once a quarter

Ensure that all personnel with access to the PBX or connected equipment have signed employee agreements including PBX-related material

Test audit mechanisms at least quarterly

Test audit computers periodically

Ensure external auditors do blind external testing

PBX Administrators

Identify the personnel or position(s) responsible for telephone usage in the PBX policy statement

Ensure that agreements with the LEC, the IXC, and the equipment vendors allow only authorized personnel to request service level changes, and to report errors

Verify all toll calls billed against PBX traffic reports

Ensure that internal PBX audits include verification that all records are in electronic form

Ensure that internal information systems auditors complete an audit of each PBX system at least once a quarter

Ensure that all personnel with access to the PBX or connected equipment have signed employee agreements including PBX-related material

Test audit mechanisms at least quarterly

Test audit computers periodically

Ensure that external auditors perform blind external testing

Site Telephone Technical Support

Clearly marks circuit numbers on channel banks, communications service units (CSUs), data service

PBX Security Responsibilities

units (DSUs), and modems

Clearly labels main distribution frames (MDF)s and intermediate distribution frames (IDF)s

Fully documents procedures for making PBX software and hardware changes, using signed checklists to record all changes as they occur

Identifies third party calls on phone bills and flag them on automated analysis

Generates and keeps full call audit records in paper and electronic forms

Follows procedures to ensure the periodic dump of all PBX parameters and automatic comparison to the previous dump; report differences to management

Follows procedures to determine the frequency of the periodic dump and comparison as a normal part of risk management

Stores PBX backups off-site; verifies the media by reading back in; and periodically tests the media on backup equipment to assure that they work properly

Ensures that a complete dump of internal parameters is reconciled with previous dumps after completion of remote maintenance

Records all transactions in an external computer system

Ensures that systems cannot redirect incoming calls from outside lines to make outside calls

Records and prints all call details

Stores records on a write once read many (WORM) disk for additional assurance

4.4.1.1 Maintenance Vulnerabilities

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

Examples of these special features include:

- **Database upload/download utility** – Allows the manufacturer to download the database from a system that is malfunctioning and examine it at their location to try to determine the cause of the malfunction
- **Database examine/modify utility** – Allows the manufacturer to remotely examine and modify a system's database to repair damage caused by incorrect configuration, design bugs, or tampering

- **Software debugger/update utility** – Permits the manufacturer to remotely debug a malfunctioning system. It also allows the manufacturer to remotely update systems with bug fixes and software upgrades.

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

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

4.4.1.2 Software Loading and Update Tampering

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

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

4.4.1.3 User Features

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

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

- Feature interaction

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

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

4.4.2 Telephone Communications

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

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

Telephone communications responsibilities are provided in the following table.

Telephone Communications Responsibilities
<p>DHS CISO</p> <p>Establishes and enforces policy relating to telephone communications</p>
<p>ISSOs</p> <p>Ensure that users are aware of the telephone communications policy</p>
<p>Users</p> <p>Adhere to the telephone communications policy that requires them not to discuss classified</p>

Telephone Communications Responsibilities
information over the telephone and to exercise care when discussing sensitive information

The following vulnerabilities of unsecured telephone systems can result in unintentional transmission of classified or sensitive information. Commonly accepted best practices dictate that users be made aware of these vulnerabilities and exercise extreme caution when discussing sensitive information on unsecured phones. Unsecured phones shall not be used to discuss classified information.

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

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

4.4.3 Voice Mail

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

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

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

Voice mail responsibilities are provided in the following table.

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

4.5 Data Communications

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

4.5.1 Telecommunications Protection Techniques

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

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

Telecommunications protection responsibilities are provided in the following table.

Telecommunications Protection Responsibilities
<p>Component CISO/ISSMs</p> <p>Advise DHS Project Managers on the selection of telecommunications protection techniques that</p>

Telecommunications Protection Responsibilities
could serve as an alternative to encryption for data transmission protection techniques
System Owners
Select the telecommunications protection techniques that meet their security needs and are consistent with DHS security policies and most cost-effective.

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

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

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

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

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

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

4.5.2 Facsimiles

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

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

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

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

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

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

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

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

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

Policy ID	DHS Policy Statements	Relevant Controls
4.5.2.a	Components shall implement and enforce technical controls for fax technology and systems (including fax machines, servers, gateways, software, and protocols) that transmit and receive sensitive information.	SC-1, SC-7, SC-8, SC-9

Policy ID	DHS Policy Statements	Relevant Controls
4.5.2.b	Components shall configure fax servers to ensure that incoming lines cannot be used to access the network or any data on the fax server.	AC-4

Facsimile responsibilities are provided in the following table.

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

4.5.3 Video Teleconferencing

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

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

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

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

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

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

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

Video teleconferencing responsibilities are provided in the following table.

Video Teleconferencing Responsibilities
<p>AOs Carefully weigh the risk associated with the use of video teleconferencing equipment connected to DHS systems prior to authorizing</p> <p>Component CISOs/ISSMs Advise DHS personnel on the selection and secure use of video teleconferencing technologies</p> <p>Supervisors Establish procedures to ensure that only authorized attendees participate in teleconferencing sessions Ensure that procedures are in place to disable video teleconferencing equipment when not in use Ensure that procedures are in place to label and store videotapes recorded during the teleconferencing</p>

Video Teleconferencing Responsibilities

ISSOs/Teleconferencing Operators

Ensure that video teleconferencing is addressed in the SP if the equipment is connected to a DHS system

Ensure that video teleconferencing equipment is disabled and secure when not in use

Ensure that appropriate transmission protections are in place commensurate with the highest sensitivity of information to be discussed when conducting a video teleconferencing session

Users

Shall not discuss information during a teleconferencing session at a higher level of classification than that established for the conference

4.5.4 Voice Over Data Networks

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

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

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

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

Information integrity is a significant security concern when using voice over data networks. Services provided by commercial entities are not directly controlled by DHS staff. Encryption of any data (including voice) that traverses these links is mandatory. The contractual arrangements with these suppliers must specify that only U.S. Citizens shall be involved in the maintenance and operation of these links.

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

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

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

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

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

Voice Over Data Networks Responsibilities
Ensure that appropriate identification and authentication controls, audit logging, and integrity controls are properly configured on every element of their voice over data networks
Facility Managers
Ensure that physical access to voice over data network elements is restricted to authorized personnel

4.6 Wireless Network Communications

Wireless network communications technologies include the following:

- Wireless systems (e.g., wireless local area networks [WLAN], wireless wide area networks [WWAN], wireless personal area networks [WPAN], peer-to-peer wireless networks, information systems that leverage commercial wireless services). Wireless systems include the transmission medium, stationary integrated devices, firmware, supporting services, and protocols
- Wireless PEDs capable of storing, processing, or transmitting sensitive information (e.g., PDAs, smart telephones, two-way pagers, handheld radios, cellular telephones, personal communications services [PCS] devices, multifunctional wireless devices, portable audio/video recording devices with wireless capability, scanning devices, messaging devices)
- Wireless tactical systems, including mission-critical communication systems and devices (e.g., include Land Mobile Radio [LMR] subscriber devices and infrastructure equipment, remote sensors, technical investigative communications systems)
- Radio Frequency Identification (RFID)

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

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

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

Policy ID	DHS Policy Statements	Relevant Controls
4.6.a	Components are prohibited from introducing new wireless network communications technologies into the enterprise unless the appropriate AO specifically approves a technology and application.	AC-18

Policy ID	DHS Policy Statements	Relevant Controls
4.6.b	Components using Public Key Infrastructure (PKI)-based encryption on wireless systems, wireless PEDs, and wireless tactical systems shall implement and maintain a key management plan approved by the DHS PKI Policy Authority.	IA-5, SC-12

Wireless communications responsibilities are provided in the following table.

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

4.6.1 Wireless Systems

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

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

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

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

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

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

Policy ID	DHS Policy Statements	Relevant Controls
	waiver or exception to policy from the DHS CISO.	
4.6.1.f	Component CISOs shall review all system applications for wireless usage, maintain an inventory of systems, and provide that inventory to the DHS CISO annually.	AC-18, PM-5
4.6.1.g	Component CISOs shall (i) establish usage restrictions and implementation guidance for wireless technologies; and (ii) authorize, monitor, and control wireless access to DHS information systems.	AC-18

Wireless system responsibilities are provided in the following table.

Wireless System Responsibilities
<p>AOs</p> <p>Approve the use of standards-based wireless system technologies</p> <p>Approve the implementation and use of wireless systems at a specified risk level during the Security Authorization Process</p> <p>Ensure that appropriate and effective security measures are included in the SP</p> <p>Component CISOs/ISSMs</p> <p>Advise System Owners and Project Managers concerning the implementation of wireless technologies</p> <p>Enforce DHS wireless systems policy</p> <p>Enforce DHS policy concerning the reporting requirements for wireless security vulnerability assessments</p> <p>System Owners/Project Managers</p> <p>Develop risk mitigation plans for prioritizing corrective actions and implementation milestones</p> <p>Develop migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless systems to DHS-compliant security architectures</p> <p>ISSOs</p> <p>Ensure that wireless systems security controls are properly implemented and configured and are addressed in the SP</p> <p>Ensure that routine security assessments of wireless systems identify unauthorized wireless devices, backdoors, and other system vulnerabilities, and enumerate vulnerabilities, risk statements, risk levels, and corrective actions</p> <p>Implement risk mitigation plans for prioritizing corrective actions and achieving implementation milestones</p> <p>Implement migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless systems to DHS-compliant security architectures</p>

Wireless System Responsibilities

System/Network Administrators

Ensure that wireless system security controls are properly implemented and configured in accordance with the SP

Ensure that routine security assessments are accomplished on wireless systems to identify rogue access points, backdoors, and other system vulnerabilities, and to enumerate vulnerabilities, risk statements, risk levels, and corrective actions

DHS Managers, Supervisors, and Employees

Adhere to DHS policy concerning the use of wireless systems to process, store, or transmit sensitive information

Adhere to DHS policy concerning the use of wireless systems in areas where sensitive information is being discussed

4.6.2 Wireless Portable Electronic Devices

Wireless PEDs include PDAs, smart telephones, two-way pagers, handheld radios, cellular telephones, PCS devices, multifunctional wireless devices, GPS 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 this Handbook's Attachment Q2, "*Wireless Portable Electronic Devices.*"

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

Personally owned PEDs are not authorized to process, transmit, or store sensitive or classified information. Personally owned PEDs may not be connected to sensitive or classified systems or networks.

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

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

turn allow administrators to remove data, update software, and log and track unauthorized removal where appropriate.

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

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

This Handbook's Attachment Q2, *Wireless Portable Electronic Devices* provides guidance for developing and implementing wireless PED security.

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.a	The use of wireless PEDs and accessory devices in areas where classified information is discussed, maintained, or distributed is prohibited unless specifically authorized in writing by the AO for the system used in the area	AC-19, PL-4
4.6.2.b	Wireless PEDs shall not be tethered or otherwise physically or wirelessly connected to the DHS-wired core network without written consent from the AO.	AC-18, AC-19
4.6.2.c	Wireless PEDs shall not be used to store, process, or transmit combinations, personal identification numbers (PIN), or sensitive information in unencrypted formats.	AC-19, IA-5, IA-7
4.6.2.d	Wireless PEDs such as BlackBerry devices and smart phones shall implement strong authentication, data encryption, and transmission encryption technologies. Portable electronic devices such as BlackBerry devices and smart phones shall be password-protected, with a security timeout period established. For BlackBerry devices, the security timeout shall be set to ten (10) minutes.	AC-19, IA-7, SC-8, SC-9, SC-13
4.6.2.e	SPs shall promulgate the provisions, procedures, and restrictions for using wireless PEDs to download mobile code in an approved manner.	SC-18
4.6.2.f	Wireless PEDs shall be operated only when current DHS TRM-approved versions of antivirus software and software patches are installed.	SI-3
4.6.2.g	Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless PED being approved for use.	SC-5 SC-7
4.6.2.h	Components shall maintain a current inventory of all approved wireless PEDs in operation.	PM-5

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.i	Wireless PEDs shall be sanitized 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.	MP-6
4.6.2.j	For legacy wireless PEDs that are not compliant with DHS information security policy a migration plan shall be implemented that outlines the provisions, procedures, and restrictions for transitioning these wireless PEDs to DHS-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception from the DHS CISO.	CA-5 CA-6
4.6.2.k	Components shall ensure that personally-owned PEDs and Government-owned PEDs not authorized to process classified information are not permitted in conference rooms or secure facilities where classified information is discussed.	AC-19, PE-18
4.6.2.l	The AO shall approve the use of Government-owned PEDs to process, store, or transmit sensitive information.	CA-6
4.6.2.m	The use of add-on devices, such as cameras and recorders, is not authorized unless approved by the AO. Functions that can record or transmit sensitive information via video, Infrared (IR), or Radio Frequency (RF) shall be disabled in areas where sensitive information is discussed.	AC-19, CM-7, PE-18, SC-7

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

Wireless Portable Electronic Device Responsibilities
<p>AOs</p> <p>Approve the use of Government-owned, DHS-approved wireless PEDs and accessory devices to connect, process, store, or transmit sensitive information</p> <p>Ensure that appropriate and effective security measures are included in the SP</p> <p>Authorize the use of Government-owned wireless PEDS and accessory devices in areas where sensitive information is discussed</p> <p>Evaluate the risk associated with authorizing wireless PEDs to connect, process, store, transmit, or access sensitive information and systems during the Security Authorization Process</p> <p>Approve/disapprove the use of mobile code (e.g., ActiveX)</p> <p>System Owners/Project Managers</p> <p>Develop risk mitigation plans for prioritizing corrective actions and implementation milestones</p> <p>Develop migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless PEDs to DHS-compliant security architectures</p>

Wireless Portable Electronic Device Responsibilities

Maintain an inventory of all approved wireless PEDs in operation

Component CISOs/ISSMs

Enforce DHS policy on the use of wireless PEDs and accessory devices in areas where sensitive information is discussed

Enforce DHS policy concerning the use of wireless PEDs and accessory devices to connect, store, process, or transmit combinations, PINs, or sensitive information

Develop procedures for implementation of strong identification, authentication, data encryption, and transmission encryption for wireless PEDs to protect sensitive information from compromise

Enforce DHS policy concerning the use of mobile code and antivirus software on wireless PEDs

Identify and establish cost-effective countermeasures to denial-of-service attacks for wireless PEDs

ISSOs

Ensure wireless PEDs are not permitted in areas where sensitive information is discussed unless authorized in writing by the AO

Enforce DHS policy concerning the use of wireless PEDs to process, store, or transmit sensitive information

Enforce DHS policy concerning the use of mobile code and antivirus software on wireless PEDs

Implement cost-effective countermeasures to denial-of-service attacks for wireless PEDs

Ensure that all information is cleared from wireless PEDs that are to be reused or surplus; ensure that all information is sanitized from wireless PEDs that are being disposed of, recycled, or returned to the owner or manufacturer (see Section 4.3.3 of this handbook for approved procedures)

Implement migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless PEDs to DHS-compliant security architectures

Enforce prohibition of add-on devices such as cameras and recorders

System/Network Administrators

Ensure that wireless PED security controls are properly implemented and configured in accordance with the SP

Ensure that routine security assessments are accomplished on wireless PEDs

DHS Managers, Supervisors, and Employees

Adhere to DHS policy concerning the use of wireless PEDs in areas where sensitive information is being discussed

Adhere to DHS policy concerning the use of wireless PEDs to process, store, transmit, or access combinations, PINs, or sensitive information

4.6.2.1 Cellular Phones

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

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

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

Cellular phone responsibilities are provided in the following table.

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

4.6.2.2 Pagers

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

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

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

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

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

Pager responsibilities are provided in the following table.

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

4.6.2.3 Multifunctional Wireless Devices

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

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

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

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

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.3.a	Functions that cannot be encrypted using approved cryptographic modules shall not be used to process, store, or transmit sensitive information.	AC-19, SC-8, SC-9, SC-12

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

Multifunctional wireless device responsibilities are in the following table.

Multifunctional Wireless Device Responsibilities
<p>AOs</p> <p>Approve the implementation of multifunctional wireless devices at an acceptable level of risk</p> <p>Ensure prior to authorization that the SP adequately addresses the protection of sensitive material accessed and stored on multifunctional wireless devices.</p> <p>Project Managers/System Owners</p> <p>Ensure that security requirements for multifunctional wireless devices are communicated to the Project Manager and system administrators</p> <p>System/ Network Administrators</p> <p>Ensure that multifunctional wireless devices are configured properly with encryption enabled to prevent unauthorized access, disclosure, damage, modification, or destruction of data</p> <p>Ensure that multifunctional wireless devices are periodically scanned for rogue access points and other vulnerabilities</p> <p>ISSOs</p> <p>Ensure that the SP addresses the protection of sensitive material accessed and stored on wireless devices</p> <p>Ensure that security requirements for multifunctional wireless devices are addressed in the SP and Rules of Behavior</p> <p>Ensure that routine security assessments are accomplished for multifunctional wireless devices to identify rogue access points, backdoors, and other system vulnerabilities, and to enumerate vulnerabilities, risk statements, risk levels, and corrective actions</p>

4.6.3 Wireless Tactical Systems

Wireless tactical systems include Land Mobile Radio (LMR) subscriber devices, infrastructure equipment, remote sensors, and technical investigative communications systems. Because they are often deployed under circumstances in which officer safety and mission success are at stake, wireless tactical systems require even greater security measures. To ensure secure tactical

communications, Components must implement strong identification, authentication, and encryption protocols designed specifically for each wireless tactical system.

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

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

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

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

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

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

Policy ID	DHS Policy Statements	Relevant Controls
4.6.3.a	AOs shall be immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents.	CM-3
4.6.3.b	Wireless tactical systems shall implement strong identification, authentication, and encryption.	IA-2, IA-7, SC-8, SC-9
4.6.3.c	Cost-effective countermeasures to denial-of-service attacks shall be identified	SC-5

Policy ID	DHS Policy Statements	Relevant Controls
	and implemented prior to a wireless tactical system being approved for use.	
4.6.3.d	Components shall maintain a current inventory of all approved wireless tactical systems in operation.	PM-5
4.6.3.e	A migration plan shall be implemented for legacy tactical wireless systems that are not compliant with DHS information security policy; The migration plan will outline the provisions, procedures, and restrictions for transitioning the legacy systems to DHS-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception from the DHS CISO, as appropriate.	---
4.6.3.f	The security configuration of LMR subscriber units shall be validated via over-the-air-rekeying (OTAR) or hard rekey using a crypto-period no longer than 180 days.	SC-12
4.6.3.g	All LMR systems shall comply with Project 25 (P25, EIA/TIA-102) security standards where applicable.	CM-2

Wireless tactical system responsibilities are provided in the following table.

Wireless Tactical System Responsibilities
<p>AOs</p> <ul style="list-style-type: none"> Approve the use of wireless tactical systems technologies Approve the implementation and use of wireless tactical systems to process, store, or transmit sensitive information at acceptable risk levels Ensure security measures are included in the SP Evaluate and submit waivers and exceptions to the DHS CISO for wireless tactical systems when compliance with DHS information security policy could potentially compromise tactical investigations, endanger personnel safety, or put the public at risk <p>System Owners/Project Managers</p> <ul style="list-style-type: none"> Implement cost-effective security measures specified in the SP including strong identification, authentication, and encryption Ensure that the AO is immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents Ensure allocation of resources to support security requirements and enforcement controls specified in the SP Ensure that tactical wireless communication security requirements are communicated to ISSOs and system administrators Develop and implement migration plans that outline provisions, procedures, and restrictions for

Wireless Tactical System Responsibilities

transitioning legacy wireless tactical systems to DHS-compliant security architectures

Maintain an inventory of all wireless tactical systems used to process, store, and transmit sensitive information

Ensure all LMR systems comply with Project 25 (P25, EIA/TIA-102) security standards where applicable

Component CISOs/ISSMs

Enforce DHS policy concerning the use of tactical communication systems to process, store, transmit, or access sensitive information

Develop and enforce DHS policy concerning mitigation measures for DoS attacks

Enforce LMR system compliance with Project 25 (P25, EIA/TIA-102) security standards

ISSOs

Ensure that the AO is immediately notified whenever any security features are disabled in response to time-sensitive, mission-critical incidents

Implement DHS policy concerning the use of tactical communication devices to process, store, transmit, or access sensitive information

Ensure that any tactical communication devices used to process sensitive information are not permitted in conference rooms or secure facilities where sensitive information is discussed without written authorization from the AO

Perform security assessments and validate the security posture of LMR subscriber units via OTAR or hard rekeying using a crypto-period no longer than one-hundred and eighty (180) days

Ensure that all information is cleared from wireless tactical systems that are to be reused or surplus

Ensure that wireless tactical systems are sanitized prior to being disposed of, recycled, or returned to the owner or manufacturer (see Section 4.3.3, for approved procedures)

DHS Managers / Supervisors

Ensure that the AO is immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents

Ensure employees are aware of DHS policy and procedure for discussing sensitive information while using tactical communication devices

Employees

Adhere to DHS policy and procedures concerning the use of tactical communication devices that access, process, store, or transmit sensitive information and systems

4.6.4 Radio Frequency Identification

RFID enables wireless identification of objects over significant distances. Because of the computing limitations of RFID tags, it often is not feasible to implement many of the security mechanisms, such as cryptography and strong authentication, that are commonly supported on personal workstations, servers, and network infrastructure devices. RFID security controls can

support Departmental and Component privacy objectives, mitigate risks to business processes, and prevent the disclosure of sensitive data.

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

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

4.7 Overseas Communications

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

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

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

[12 FAM 610, *Organization and Purpose of Computer Security \(COMPUSEC\)*](#)

[12 FAM 620, *Unclassified Automated Information Systems*](#)

[12 FAM 630, *Classified Automated Information Systems*](#)

[12 FAM 640, *Domestic and Overseas Automated Information Systems Connectivity*](#)

[12 FAM 650, *I Components*](#)

12 FAM 660, *Communications Security* (this section has been designated Sensitive—NOFORN and is not available via the Internet; contact the Department of State to obtain a hardcopy version).

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

Overseas communications responsibilities are provided in the following table.

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

4.8 Equipment

Equipment security encompasses workstations, laptops, other mobile computing devices, personally owned equipment, and the maintenance of these items. This section addresses the use

and maintenance of computer equipment and stresses the importance of individual accountability in protecting these resources.

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

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

- Workstations must be adequately protected from theft.
- Only licensed and approved operating systems and applications may be used on DHS workstations.
- All default vendor or factory set administrator accounts and passwords shall be changed before installation or use.
- All equipment shall be marked with the highest level of classification of information that has ever been processed or stored on the device, if there are any devices authorized for processing National Security information in the vicinity.
- Equipment must be housed in facilities authorized to process sensitive information.

4.8.1 Workstations

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

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

Workstation responsibilities are provided in the following table.

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

4.8.2 Laptop Computers and Other Mobile Computing Devices

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

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

Mobile computing devices cannot be connected to DHS networks or systems unless such connections are authorized to the network or system. The security plan must identify the devices that can be used to access the network or system, the purposes for the access, and the security controls to be employed for the connection. Any laptop computers or other mobile computing devices that process sensitive data (whether or not they are connected to a DHS network) must employ virus protection. All removable media must be scanned prior to use to ensure it is free of malware.

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

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

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

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

Laptop Computer and Other Mobile Computing Device Responsibilities
<p>DHS CISO Establishes DHS policy regarding the use of mobile computing devices</p> <p>Component CISOs/ISSMs Enforce DHS policy regarding the use of mobile computing devices Provide technical expertise and evaluate the effectiveness of encryption methods for mobile computing devices</p> <p>System/Network Administrators Provide technical expertise and evaluate the effectiveness of encryption methods for mobile computing devices Ensure that encryption technology is installed and properly configured on mobile computing devices Assist ISSOs in implementing technical requirements for mobile computing devices</p> <p>ISSOs Ensure that security of mobile computing devices is adequately addressed in the security plan Ensure users are aware of their responsibility to adhere to the Rules of Behavior for mobile computing devices Ensure that users are trained in the use of encryption for mobile computing devices Ensure that physical security controls are in place for mobile computing devices</p>

Laptop Computer and Other Mobile Computing Device Responsibilities
Ensure the unique requirements for connection of mobile computing devices to the network are addressed in the Security Plan
Ensure that encryption methods employed on mobile computing devices provide the protection required in the security plan
Users
Obtain written approval of the office director before taking mobile computing device overseas
Comply with the Rules of Behavior for mobile computing devices
Utilize encryption technology provided for mobile computing devices
Physically secure mobile computing devices when not in use
Read and adhere to the mobile computing device policies and procedures in this section and in Rules of Behavior
Make supervisors and managers aware of any problems encountered in implementing mobile computing device guidance and procedures

4.8.3 Personally Owned Equipment and Software

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

Components shall conduct semiannual reviews of all equipment and software to ensure that only Government-licensed software and equipment are being used, or that appropriate exceptions have been documented.

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

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

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

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

Personally Owned Equipment and Software Responsibilities
<p>AOs Carefully evaluate the risk associated with authorizing the use of personally owned equipment or software</p> <p>Component CISOs/ISSMs Enforce DHS policy prohibiting the use of personally owned equipment to connect, process, store, or access sensitive information and systems</p> <p>ISSOs Enforce DHS policy prohibiting the use of personally owned equipment to connect, process, store, or access sensitive information and systems Conduct reviews, at least semiannually, of all equipment and software in their respective offices to ensure that only Government-licensed software and equipment are being used Ensure that Rules of Behavior address policy regarding the use of personally owned equipment and software Ensure that security awareness sessions address policy regarding the use of personally owned equipment and software</p> <p>Users Adhere to DHS policies prohibiting the use of personally owned equipment and software</p>

4.8.4 Hardware and Software

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

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

Baselines were developed using a variety of security guidelines from the NSA, the Defense Information Systems Agency (DISA), NIST and other Federal agencies, and from vendor

recommendations. . The principle reference used was NIST SP 800-70: “Security Configuration Checklists Program for Information Technology (IT) Products – Guidance for Checklists Users and Developers.”), These baselines represent the minimum configuration requirements; Components are authorized to implement more rigorous configuration guides. If unable to meet the published configuration baselines, a waiver or exception is required.

Policy ID	DHS Policy Statements	Relevant Controls
4.8.4.a	Components shall ensure that DHS information systems follow the hardening guides for operating systems and the configuration guides for applications promulgated by the DHS CISO. <i>DHS Sensitive Systems Handbook 4300A</i> , Enclosure 1, includes the DHS Secure Baseline Configuration Guides.	CM-2, CM-6
4.8.4.b	Components shall limit access to system software and hardware to authorized personnel.	AC-3, CM-5
4.8.4.c	Components shall test, authorize, and approve all new and revised software and hardware prior to implementation in accordance with their Configuration Management Plan.	CM-2, CM-3
4.8.4.d	Components shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches, and eliminating or disabling unnecessary services.	CM-3, RA-5
4.8.4.e	Components shall ensure that maintenance ports are disabled during normal system operation and enabled only during approved maintenance activities.	MA-1
4.8.4.f	System libraries shall be managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.	SI-7
4.8.4.g	Components shall develop maintenance policy and procedures.	MA-1
4.8.4.h	If cleared maintenance personnel are not available, a trusted DHS employee with sufficient technical knowledge to detect and prevent unauthorized modification to the information system or its network shall monitor and escort the maintenance personnel during maintenance activities. This situation shall only occur in exceptional cases. Components shall take all possible steps to ensure that trusted maintenance personnel are available.	MA-5
4.8.4.i	Maintenance using a different user’s identity may be performed only when the user is present. The <i>user</i> shall log in and observe the maintenance actions at all times. <i>Users shall not share their authentication information with maintenance personnel.</i>	MA-5

Hardware and software responsibilities are provided in the following table.

Hardware and Software Responsibilities

DHS CISO

Approves secure baseline configuration guides

Component CISO/ISSMs

Provide guidance in the preparation of secure baseline configuration guides for hardware and software; DHS CISO approves secure baseline configuration guides

AO

Ensures new hardware and software products have been approved and documented in the Security Authorization Process documentation

ISSOs

Ensure that adequate security measures are in place to protect access to hardware and software

Ensure that new hardware and software products have been approved in accordance with the configuration management plan prior to installation

Network/ System Administrators

Ensure that hardware and software are properly secured

Ensure that maintenance ports are disabled when not in use

Ensure that unnecessary services are disabled when possible

Scan system periodically to identify vulnerabilities and take corrective actions to reduce them

Test software security patches on a non-live system prior to implementation on active production systems

Ensure that new hardware and software products have been approved in accordance with the configuration management plan prior to installation

Facility Managers

Ensure adequate physical security measures are in place to protect access to hardware and software

Ensure that access control policy is enforced

System Owners/Project Managers

Ensure that the installation of hardware and software products meets the configuration requirements specified in applicable DHS secure baseline configuration guides

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

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

- Involves minimal additional expense to the Government
- Is performed on the employee's non-work time
- Does not reduce productivity or interfere with DHS missions or operations
- Does not violate the *Standards of Ethical Conduct for Employees of the Executive Branch*

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

- Use of Internet sites resulting in an additional charge to the Government
- Obtaining, viewing, or transmitting sexually explicit material or other material inappropriate to the workplace
- Use for other than official Governmental business that results in significant strain on Department computer systems (e.g., mass mailings or sending or downloading large files such as programs, pictures, video files, or games)
- Any otherwise prohibited activity, such as sending out solicitations or engaging in political activity prohibited by the Hatch Act

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

Inappropriate use is considered a security incident. Depending on its severity, the incident may be deemed a security violation and, as such, be reportable under the DHS SOC provisions of Section 4.9 and of this Handbook's Attachment F, "Incident Response and Reporting."

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

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

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

Contractors are not authorized to use Government office equipment or systems for personal use under any circumstances, unless limited personal use is specifically permitted by their contract. When limited use is authorized, contractors shall be governed by the limited personal use policies of this section.

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

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

Personal Use of Government Office Equipment and DHS Systems Responsibilities
<p>Human Capital Office</p> <p>Establishes DHS policy regarding personal use of Government resources</p>
<p>DHS CIO/CISO</p> <p>Provide policy and guidance concerning appropriate use of computer resources</p> <p>Establish and implement appropriate enforcement policies for noncompliance with computer resource usage policies</p>
<p>Component CISOs/ISSMs</p> <p>Ensure that controls, including awareness training, are in place to minimize or prevent unauthorized use of Government resources</p>
<p>Supervisors</p> <p>Enforce personal use policies, including remedial training and other sanctions</p> <p>Promptly report unauthorized use of Government resources in accordance with DHS incident reporting procedures (see DHS 4300A Attachment F)</p>
<p>ISSOs, Network/System Administrators</p> <p>Remind users of their system responsibilities and the potential penalties for misuse of system resources</p> <p>Remind users that they do not have any right to or expectation of privacy while using Government office equipment DHS systems, including Internet and email services</p>
<p>Users</p> <p>Be aware of the personal use policies described in this section of the handbook and in other references provided by DHS security officials, including the Standards of Ethical Conduct for Employees of the Executive Branch</p> <p>Adhere to personal use policies established in this section and in other references provided by DHS security officials</p> <p>Promptly report unauthorized use of Government resources in accordance with DHS incident reporting procedures (see Attachment F to this Handbook.)</p> <p>Be aware of and understand the disciplinary actions associated with violations of information security policy, including the unauthorized use of Government resources</p> <p>Shall <i>not</i> have any expectation of privacy in the use of Government computers or computer systems</p>
<p>Contractors and non-DHS Employee Users</p> <p>Understand and abide by the personal use provisions of the contract or memorandum of agreement with DHS</p>

4.8.6 Wireless Settings for Peripheral Equipment

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

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

4.9 Department Information Security Operations

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

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

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

The effects of security incidents can range from embarrassment to interruption of service to inability to function, and, potentially, to loss of human life. A significant concern is that hostile individuals or foreign states could severely damage or disrupt critical operations, resulting in harm to the public welfare. DHS maintains a security incident reporting and handling capability to help combat the disruptive short and long-term effects of security incidents.

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

distinction is to be made between suspected and confirmed incidents. US-CERT forwards all agency reports to the appropriate Identity Theft Task Force point of contact within one (1) hour of notification by an agency.

Policy ID	DHS Policy Statements	Relevant Controls
4.9.a	It is the policy of DHS that employees, contractors, or others working on behalf of DHS have no privacy expectations associated with the use of any DHS network, system, or application. This policy is further extended to anyone who is granted account access to any network, system, or application in use in the Department. By completing the account login process the account owner acknowledges their consent to monitoring.	AC-8, PL-4
4.9.b	Component SOCs and the HSDN SOC shall be operationally subordinate to the DHS SOC, which shall provide them operational oversight and guidance.	IR-1
4.9.c	The DHS SOC or Component SOCs shall lead the coordination and administration of Department and Component policy enforcement points, such as firewalls.	SC-7
4.9.d	The DHS SOC shall implement the Department logging strategy, coordinated with Component SOCs, to enable endpoint visibility and Departmental situational awareness.	---
4.9.e	All SOCs shall have the capability to process intelligence information at the collateral level or above. The DHS SOC and Component SOCs shall have the ability to process SECRET level information continuously and shall have the capability to receive Top Secret / Sensitive Compartmented Information (TS/SCI) information.	IR-4
4.9.f	SOCs shall ensure that personnel are appropriately cleared to access Joint Worldwide Intelligence Communications System (JWICS). SOC managers are free to determine the number and type of personnel to be cleared, but at least one cleared person shall be available per shift. (This person may be on call.) A Government officer shall be available continuously for incident response and management.	IR-4
4.9.g	All Department SOCs shall establish and maintain a forensic capability as outlined in the DHS Security Operations Concept of Operations (SOC CONOPS).	IR-7
4.9.h	Department information security operations shall provide a vulnerability management capability. DHS SOC provides Information Security Vulnerability Management (ISVM) messages and vulnerability assessment capabilities. Component SOCs shall develop a robust vulnerability management capability to compliment the DHS SOC.	SI-5
4.9.i	Component CISOs shall ensure that the DHS CISO is kept apprised of all	SI-5

Policy ID	DHS Policy Statements	Relevant Controls
	pertinent matters involving the security of information systems and that security-related decisions and information are distributed to the ISSOs and other appropriate persons.	
4.9.j	Component SOC's shall report operationally to their respective Component CISO. Each CISO shall exercise oversight over their Component's information security operations functions, including the Component SOC's.	IR-1
4.9.k	The DHS SOC shall report operationally to the DHS CISO.	
4.9.l	The NOC/SOC shall be under the direction of a Government employee who shall be present at all times.	

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

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

Security Incident Response and Reporting Responsibilities
<p>Users</p> <p>Promptly report information security incidents in accordance with DHS incident reporting procedures (see Attachment F to this Handbook)</p>

4.9.1 Security Incidents and Incident Response and Reporting

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

Policy ID	DHS Policy Statements	Relevant Controls
4.9.1.a	Components shall establish and maintain a continuous incident response capability.	IR-1
4.9.1.b	Component SOC's shall report significant incidents to the DHS SOC by via SOCOOnline (https://soconline.dhs.gov) as soon as possible but not later than one hour after discovery of the incident. Other means of reporting, such as calling (1-877-DHS1NET) or emailing (DHS.SOC@dhs.gov) are acceptable, but the Component shall <u>positively verify</u> that notification is acknowledged by the DHS SOC.	IR-6
4.9.1.c	Significant HSDN incidents shall be documented with an initial detailed report to the HSDN Government Watch Officer and to the DHS SOC via secure communications as soon as possible but not later than one hour after discovery of the incident. Subsequent updates and status reports shall be provided to the HSDN SOC and to the DHS SOC via secure email every twenty-four (24) hours and whenever new information is discovered. Significant incidents are reported individually and shall not be reported in the monthly summary report.	IR-6
4.9.1.d	Components shall report minor incidents via the DHS SOC portal (https://soconline.dhs.gov) within 24 hours of validation. Components without portal access shall temporarily report minor incidents via email to dhs.soc@dhs.gov . HSDN incidents or incidents involving SECRET information shall be documented in a summary report and sent via secure email to the HSDN SOC.	IR-6
4.9.1.e	DHS personnel shall follow DHS CISO procedures for detecting, reporting, and responding to information security incidents in accordance with the DHS SOC CONOPS. Reports shall be classified at the highest classification level of the information contained in the document. Unsanitized reports shall be marked and handled appropriately.	IR-1
4.9.1.f	If a DHS Component has no incidents to report for a given week, a "No Incidents" report shall be sent using SOCOOnline.	IR-6

Policy ID	DHS Policy Statements	Relevant Controls
4. 9.1.g	The DHS SOC shall report incidents to the United States Computer Emergency Readiness Team (US-CERT) in accordance with the DHS SOC CONOPS. Components shall not send incident reports directly to US-CERT.	IR-6
4. 9.1.h	The DHS SOC shall receive classified spillage incident reports, and support the DHS CSO for containment and cleanup. All classified spillages are significant incidents.	IR-6
4. 9.1.i	The DHS SOC shall maintain information security “playbooks” that implement procedures and provide guidance on how to respond rapidly to developing incidents.	IR-1
4. 9.1.j	The DHS SOC shall respond to detected faults, attacks, events, or incidents and communicate incident reports to external organizations that may be affected.	IR-1
4. 9.1.k	Components shall maintain a full SOC capability or outsource SOC capability to the DHS SOC. The DHS SOC shall provide SOC services to Components in accordance with formal agreements. Information regarding incident response capability is available in Attachment F to the <i>DHS 4300A Sensitive Systems Handbook</i> .	IR-7
4. 9.1.l	Components shall develop and publish internal computer security incident response plans and incident handling procedures, and provide copies to the SOC. Each procedure shall include a detailed Configuration Management (CM) process for modification of security device configurations.	IR-1
4. 9.1.m	Component Heads shall ensure that corrective actions are taken when security incidents and violations occur, and shall hold personnel accountable for intentional misconduct.	IR-1
4. 9.1.n	The DHS SOC shall monitor and report incident investigation and incident remediation activities to the DHS Chief Information Officer (CIO) and CISO in accordance with the DHS SOC CONOPS until the incident is closed.	IR-5
4. 9.1.o	The DHS CISO shall determine the frequency and content of security incident reports.	IR-6
4. 9.1.p	The Component SOC shall report incidents only to the DHS SOC and to no other external agency or organization.	IR-6
4. 9.1.q	The DHS CISO shall publish Incident Response Testing and Exercise scenarios as required.	IR-1
4. 9.1.r	The Component CISO for each Component providing an incident response capability shall ensure Incident Response Testing and Exercises are conducted	IR-3

Policy ID	DHS Policy Statements	Relevant Controls
	annually in coordination with the DHS CISO.	

4.9.1.1 DHS SOC Organization

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

4.9.1.2 Logging and Monitoring

The DHS SOC shall maintain visibility into security operations by using logging and monitoring. The DHS SOC logging strategy can be broken into two main elements: real-time Security Incident Management (SIM) logging and monitoring; and archive logging designed for offline processing and later retrieval in the event of a security incident.

Effective DHS security event logging capability requires SOC and element asset integration, requisite event visibility, retention, storage considerations and direction for elements to provide logging events into the DHS SOC toolset and relevant security policy reference.

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

4.9.1.3 Authority and Management

Security operations oversight and management is inherently a Governmental responsibility, not one that can be outsourced solely to contractors. While a Component SOC may contract for security operation capabilities, the responsibility and ultimate authority must lie with a Government employee. The Governmental authority, commonly assigned as a Federal SOC manager, and one or more Watch Officers, must have the ability to make decisions on behalf of the Government in response to the ever-changing cyber threat landscape. This is not an authority that can be delegated.

The Federal SOC manager and at least one Government Watch Officer must be cleared to TS/SCI. Ideally all Watch Officers will be TS/SCI cleared. Such clearance is necessary to receive threat intelligence updates at Top Secret (TS) and above.

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

4.9.1.4 Forensics

Forensics is “...the examination of computer systems and the digital information created and stored on such systems to extract and analyze evidence in support of an investigation.”¹¹

Whenever a system compromise occurs, a computer forensic investigation will reveal whether or not the network or system has become a target of criminal action or has been used in the commission a crime. Forensic investigation can protect against future incidents by revealing vectors and methods of intrusion, thus suggesting measures which can be taken to protect against future incidents.

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

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

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

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

¹¹ *IT Security Architecture Guidance Volume 2*

*Table 2 – Forensic Investigations Tiers***4.9.1.5 Vulnerability Management**

Vulnerability management is a combination of detection, assessment, and mitigation of systematic weaknesses. Vulnerabilities may be revealed by a number of sources, including reviews of previous risk assessments; audit reports; vulnerability lists; security advisories; and system security testing (such as automated vulnerability scanning and Security Control Assessment).

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

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

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

4.9.1.6 Information Security Vulnerability Management

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

ISVM messages to Components can be of three forms:

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

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

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

Table 3 – ISVM Requirements

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

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

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

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

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

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

4.9.2 Law Enforcement Incident Response

The DHS SOC shall notify the DHS Chief, Internal Security and Investigations Division, Office of Security (CISID-OIS) whenever an incident requires law enforcement involvement. Law

enforcement shall coordinate with the DHS SOC, the CISID-OIS, the Component, and other appropriate parties whenever a crime is committed or suspected.

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

4.9.3 Definitions and Incident Categories

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

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

- Use of Internet sites that result in an additional charge to the Government
- Obtaining, viewing, or transmitting sexually explicit material or other material inappropriate to the workplace, which might be considered to contribute to a hostile work environment for some employees
- Use for other than official Governmental business that results in significant strain on Department computer systems (e.g., mass mailings or sending or downloading large files such as programs, pictures, video files, or games)
- Any otherwise prohibited activity, such as sending out solicitations or engaging in political activity prohibited by the Hatch Act

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

- Unauthorized attempts to gain access to information

- Introduction of malicious code or viruses into an information system
- Loss or theft of computer media

Categories of incidents include the following:

- **Unauthorized Access (Intrusion):** Unauthorized access includes all successful unauthorized accesses and suspicious unsuccessful attempts
- **Denial of Service:** Denial of service attacks include incidents that affect the availability of critical resources such as email servers, Web servers, routers, gateways, or communications infrastructure
- **Malicious Logic:** Malicious logic includes active code such as viruses, Trojan horses, worms, and scripts used by crackers/hackers to gain privileges and/or information, capture passwords, or modify audit logs to hide unauthorized activity
- **Misuse:** Misuse occurs when a user violates Federal laws or regulations and/or Department policies regarding proper use of computer resources; installs unauthorized or unlicensed software; or accesses resources or privileges that are greater than those assigned
- **PII incident:** PII incidents are suspected and confirmed breaches of personally identifiable information in electronic or physical form
- **Probes and Reconnaissance Scans:** These include probing or scanning networks for critical services or security weaknesses; This category also includes nuisance scans
- **Classified System Incident:** Any incident that involves a system used to process national security information
- **Alteration/Compromise of Information:** Any incident that involves the unauthorized altering of information, or any incident that involves the compromise of information
- **Multiple Component:** Multiple component incidents are those considered significant incidents in more than one of the above categories

4.10 Documentation

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

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

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

Policy ID	DHS Policy Statements	Relevant Controls
4.10.a	Components shall ensure that information systems and networks are appropriately documented in such a way as to allow others to understand system operation and configuration.	CM-8
4.10.b	System Owners shall update system documentation annually or whenever significant changes occur. Changes that may require updates include: <ul style="list-style-type: none"> • New threat information • Weaknesses or deficiencies discovered in currently deployed security controls after an information system breach • A redefinition of mission priorities or business objectives resulting in a change to the security category of the information system • A change in the information system (e.g., adding new hardware, software, or firmware; or establishing new connections) or the system's environment of operation 	CM-3, CM-8, SA-5
4.10.c	Documentation shall be kept on hand and shall be accessible to authorized personnel (including auditors) at all times.	CM-3 SA-5
4.10.d	System documentation may be categorized as Sensitive if deemed appropriate by the Component CISO/ISSM. This category shall not be used as a means of restricting access to auditors or other authorized personnel.	CM-3

Documentation responsibilities are provided in the following table.

Documentation Responsibilities
<p>Component CISOs/ISSMs Ensure that security issues are formally documented and tracked during the SELC process</p> <p>Project Managers/ISSOs Ensure that change control procedures are documented and implemented for all proposed configuration changes to systems</p> <p>Ensure that all proposed configuration changes to operating systems, operating system security features, applications, critical system files, and system devices are formally approved and documented</p>

Documentation Responsibilities
<p>prior to the change being implemented</p> <p>Maintain a capability to quickly approve and implement time-sensitive security patches in reaction to late-breaking notification of security vulnerabilities identified by the DHS SOC</p> <p>Ensure that all approved changes to the configuration baseline are documented and reviewed for accuracy, and that records are maintained for each system for both current and all previous configurations</p> <p>Ensure that formal system configuration reviews are performed</p> <p>Ensure that accurate system documentation and configuration logs are maintained to reflect current and prior configuration baselines</p>

4.11 Information and Data Backup

Adhering to requirements regarding data backups can significantly reduce the risk that data will be compromised or lost in the event of a disaster or interruption of service. A Backup Operations Plan must be included in the Contingency Plan, as discussed in Section 3.5.2, “Information Technology Contingency Planning.”

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

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

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

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

- Space requirements of the recovery site
- Power and environmental requirements
- Backup documentation requirements

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

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

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

Policy ID	DHS Policy Statements	Relevant Controls
4.11.a	The policies in this document, including Security Authorization Process requirements, apply to any devices that process or host DHS data.	---
4.11.b	Component ``CISOs/ISSMs shall determine whether or not automated process devices shall be included as part of an information system’s Security Authorization Process requirements.	---

Information and data backup responsibilities are provided in the following table.

Information and Data Backup Responsibilities
<p>Component CISOs/ISSMs</p> <p>Establish and enforce backup policy</p> <p>Provide technical expertise and evaluate the effectiveness of backup approaches</p>

Information and Data Backup Responsibilities

Security Control Assessors

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

System Owners

Ensure that a backup strategy and procedures are established, implemented, and tested in accordance with the Contingency Plan

System/Network Administrators

Ensure that regular (daily, weekly, monthly) backups are performed in accordance with system requirements

Ensure that analyses are performed to determine the volume of data to be backed up, frequency of data modifications and updates, and access needs of the user community

Maintain a proper rotation strategy for backups

Ensure that all backup tapes are properly labeled in accordance with the highest data sensitivity level assigned to the system

Ensure that on-site and off-site backup storage locations are available

Ensure that on-site backups are stored in fire and water-proof containers

Ensure that at least one backup copy of system software is retained off-site

ISSOs

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

Ensure that the Backup Operations Plan is tested *at least annually* and more frequently if the risk and magnitude of loss is sufficient to warrant doing so

Ensure that timely corrective actions are taken to address deficiencies discovered during testing

Ensure that on-site and off-site backup storage locations are available, that on-site backups are stored in fire and water-proof containers and that at least one back-up copy of system software is retained off-site

Ensure that users are apprised of their responsibility to back up any sensitive data residing on their hard drives

Review the Contingency Plan as part of the authorization process

Ensure users and system administrators understand their responsibilities and are aware of negative impacts that can result from failing to adequately back up critical data

Ensure the Contingency Plan, including backup procedures, is tested at least annually and that timely corrective action is taken to address deficiencies discovered during testing

Ensure that all testing is formally documented and ensure that records are maintained as part of the system history

Users

Understand the critical nature of backing up sensitive data

Information and Data Backup Responsibilities
Never keep critical data on individual hard drives unless a backup copy exists, preferably on the network
Keep supervisors apprised of projects in which critical data may not be adequately backed up

4.12 Converging Technologies

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

The use of nontraditional information systems elements without appropriate safeguards presents risks to DHS organizations in part because these devices are typically not thought of as information systems.

Wireless devices must be secured as specified in Section 4.6, Wireless Communications. Copiers with the capability to process sensitive documents must be secured in the same manner as facsimile machines (see Section 4.5.2). Sanitization of media included in copiers (or other devices) must be carried out in the manner prescribed in Section 4.3.3, Media Sanitization and Disposal. If the device is a multifunction device, the fax functions must be secured in the same manner as stand-alone fax machines. Printing functions must be secured in accordance with the provisions in Section 4.3.4, Production, Input/Output Controls.

HVAC, fire suppression, and power equipment (including emergency power backup) shall be secured in accordance with the requirements specified for PBXs, as described in Section 4.4.1. If these do not have internal auditing functions, manual audit/access logs are to be maintained by a trusted employee who accompanies any individual who performs maintenance, upgrade or repair on the indicated systems.

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

Policy ID	DHS Policy Statements	Relevant Controls
4.12.a	The policies in this document apply to any networked devices that contain Information Technology (IT), including copiers, facsimile machines, and alarm control systems.	---
4.12.b	Components shall ensure that network printers and facsimile machines are updated to the latest version of their firmware/software at least annually.	CM-2

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

Responsibilities related to converging technologies are provided in the following table.

Converging Technologies Responsibilities
<p>ISSOs</p> <p>Ensure that nontraditional information system elements connected to sensitive systems meet the security requirements detailed in this handbook and are assessed and authorized for that purpose</p> <p>Ensure media storage devices included in copiers, fax machines, printers, etc., are properly sanitized before leaving DHS control</p> <p>Ensure audit logs are maintained and reviewed for nontraditional information system elements that store or process sensitive information</p>

Converging Technologies Responsibilities**Network/System Administrators**

Protect and monitor network connections to nontraditional information system devices such as fax machines and copiers

Facility Managers

Notify and coordinate with the ISSO when facility systems (e.g., HVAC and alarm systems) require connectivity to sensitive systems

Ensure proper physical security is afforded to infrastructure equipment that processes, stores, or connects to a sensitive system

5.0 TECHNICAL CONTROLS

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

Technical controls are security controls that a computer system executes. These controls can provide automated protection from unauthorized access or misuse; facilitate detection of security violations; and support security requirements for applications and data.

5.1 Identification and Authentication

Identification is the process of telling a system the identity of a subject. Usually this is done by entering a name or presenting a token to the system via a Smart Card. The identity of each user must be established prior to authorizing access to the system, and each system user must have his or her own unique User ID.

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

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

DHS systems must be designed to ensure that each user is authenticated prior to being allowed access. Concurrent logins to the same system or application using the same authentication credentials are not allowed, unless a specific business or operational need is documented and approved by the AO.

Policy ID	DHS Policy Statements	Relevant Controls
5.1.a	Components shall ensure that user access is controlled and limited based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.	IA-1, IA-2
5.1.b	For information systems requiring authentication controls, Components shall ensure that the information system is configured to require that each user be authenticated before information system access occurs.	IA-1, IA-2
5.1.c	For systems with low impact for the confidentiality security objective, Components shall disable user identifiers after ninety (90) days of inactivity; for systems with moderate and high impacts for the confidentiality security objective, Components shall disable user identifiers after forty-five (45) days of inactivity.	IA-4
5.1.d	Department of Homeland Security (DHS) users shall not share identification	IA-5

Policy ID	DHS Policy Statements	Relevant Controls
	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.	
5.1.e	All user authentication materials shall be treated as sensitive material and shall carry a classification as high as the most sensitive data to which that user is granted access using that authenticator.	IA-7
5.1.f	Components shall implement strong authentication on servers, for system administrators and personnel with significant security responsibilities, within six (6) months of the Component’s implementation of Homeland Security Presidential Directive (HSPD) HSPD12.	IA-2
5.1.g	Where available, PIV credentials shall be used as the primary means of logical authentication for DHS sensitive systems.	---

Identification and authentication responsibilities are provided in the following table below.

Identification and Authentication Responsibilities
<p>DHS CISO</p> <p>Establishes and enforces identification and authentication policy</p> <p>Provides technical expertise and evaluates the effectiveness of identification and authentication approaches</p> <p>Assesses technology opportunities that have the potential to enhance compliance with identification and authentication requirements</p> <p>Security Control Assessors</p> <p>Ensure that systems limit user access based on the identification and authentication of each user prior to system access.</p> <p>System Owners/Project Managers</p> <p>Ensure that adequate resources are budgeted for information assurance; assess identification and authentication technology opportunities for potential application to DHS systems</p> <p>System/Network Administrators</p> <p>Ensure that the system identifies every user as unique</p> <p>Secure and administer privileged accounts using authentication technology stronger than passwords</p> <p>ISSOs</p> <p>Brief users on identification and authentication procedures and protection requirements</p> <p>Monitor and enforce compliance with identification and authentication requirements</p>

Identification and Authentication Responsibilities
Perform system audits to verify compliance
Users
Comply with identification and authentication guidance, specifically guidance pertaining to password management (see Section 5.1.1.1)
Report violators of security policies

5.1.1 Passwords

The least expensive method for authenticating users is a password system in which authentication is performed each time a password is used. More sophisticated authentication techniques, such as Smart Cards and biological recognition systems (e.g., retina scanner, handprint, voice recognition), shall be cost-justified through the risk assessment process.

A password is a sequence of characters used for authentication purposes. Passwords are often used to authenticate the identity of a system user and, in some instances, to grant or deny access to private or shared data.

Passwords provide a reasonable degree of authentication and are one of the most common methods used for controlling system access. Passwords are important because they are often the first line of defense against intruders or insiders who may be trying to obtain unauthorized access to a DHS system. To be used effectively, policies requiring strong passwords must be implemented, and users and system administrators must follow DHS password guidelines.

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

Policy ID	DHS Policy Statements	Relevant Controls
5.1.1.f	Components shall ensure that all passwords are stored in encrypted form.	IA-5

The use of a personal password by more than one individual is prohibited throughout DHS. It is recognized, however, that, in certain circumstances such as the operation of crisis management or operations centers, watch team and other duty personnel may require the use of group User IDs and passwords.

5.1.1.1 Selecting Strong Passwords

Users must select well-constructed passwords. The following password guidelines shall be used in order to ensure that passwords comply with DHS requirements. For guidance on how to change passwords for a variety of DHS systems, see Attachment L to this Handbook, *Password Management*.

Required Action	Benefit Gained
Passwords shall: Be at least 8 characters in length. Contain a combination of alphabetic, numeric, and special characters. Not be the same as any of the user's previous 8 passwords	These requirements make it more difficult for a password guesser to obtain passwords. They increase the set of combinations that must be guessed and provide a mixture to defeat a dictionary attack.
Passwords shall not contain any dictionary word.	Prevents dictionary type of attacks.
Passwords shall not contain any proper noun or the name of any person, pet, child, or fictional character. Passwords shall not contain any employee serial number, Social Security number, birth date, phone number, or any information that could be readily guessed about the creator of the password.	Helps prevent a password guess based on a hacker's personal knowledge of the user.
Passwords shall not contain any simple pattern of letters or numbers, such as "qwerty" or "xyz123".	Protects against dictionary attacks
Passwords shall not be any word, noun, or name spelled backwards or with a single digit appended, or with a two-digit "year" string, such as 98xyz123.	Protects against dictionary attacks
Pass phrases, if used in addition to or instead of passwords, should follow the same guidelines.	Consistent application of guidelines.
Passwords shall not be the same as the User ID.	Risk of unauthorized access is reduced, as hackers initially try "obvious" passwords such as username and User ID.

5.1.1.2 Results of Weak Passwords

Hackers have access to a variety of password-cracking tools. Weak passwords may allow internal or external users or hackers to gain unauthorized access to DHS systems.

Brute force attacks involve manual or automated attempts to guess valid passwords. There are numerous password-guessing programs available on the Internet. Most hackers have a “password hit list,” which is a collection of default passwords automatically assigned to various system accounts. For example, the default password for the guest account in most UNIX systems is “guest.”

Many hackers will try to guess passwords using a user’s personal information, such as birth date, name of spouse or children, pets, employee ID number, etc. Often, hackers will practice what they call “social engineering,” which involves talking with employees to find out things about the systems in their office, and, more importantly, personal information that will help them guess passwords.

Users tend to choose passwords that are easy to remember such as the name of a family member or pet, a birth date, or a word that may mean something to the user. These types of passwords are the easiest for others to guess.

People are the key to constructing good passwords. Poorly constructed passwords make it easier for a hacker to crack the password. The longer it takes hackers to get a password, the more likely they are to move on to other methods of gaining access to the system.

It should be noted that many computer systems use auditing features that keep a record of actions initiated by the users while on the system. Once a hacker cracks a password and gains access to the system using the appropriate User ID, the system audit logs shall record that the User ID was used in taking harmful actions on the system. Authentication is the basis for control and accountability of the users on the system.

5.1.1.3 System Administrator Responsibilities

System administrators should follow the DHS password guidelines in the following table to ensure that password settings are in compliance with DHS requirements.

A secure method for distribution of passwords is also necessary. Administrators must verify an individual’s identity prior to communicating account or password information.

Required Action	Benefit Gained
Do not store passwords in a clear text file.	Avoids situation where convenience and speedy login are achieved at the expense of security.
Passwords shall be changed or expire in 180 days or less.	By increasing password variability, reduces the likelihood of unauthorized penetrations
Do not enable a password to be reused for at least 8 iterations.	By increasing password variability, reduces the likelihood of unauthorized penetrations

Required Action	Benefit Gained
Allow only one user per account; never share User IDs or passwords.	Provides user accountability.
Never assign a login account a password that is the same string as the User ID or that contains the User ID.	Eliminates the hackers' first line of attack, which is to try User ID as the password once they get a telnet prompt.
Never install a guest/guest account.	Prevents penetration via certain well-known vulnerabilities in some User Datagram Protocol User Datagram Protocol (UDP) services.
Deactivate unused accounts monthly. For systems with a low impact for the confidentiality security objective, consider an account unused if no login has occurred in 90 days. For systems with a moderate or high impact for the confidentiality security objective, consider an account unused if no login has occurred in 45 days.	Prevents a formerly authorized user from continuing to use the host.
No accounts will be named anonymous, ftp, telnet, www, host, user, bin, nobody, etc.	Avoids accounts commonly attacked via the password-guessing method: e.g., ftp/ftp.
The manager or owner of the host shall revalidate the list of User IDs at least annually.	Best security practice to clean out User IDs of ex-employees and to verify which User IDs are valid.
Never set any password equal to the null string, which is equivalent to no password at all.	Follows best security practices.

Privileged accounts shall be secured by authentication technology stronger than that based only on a User ID and password. All actions taken by remote privileged users must also be logged for auditing purposes and shall be encrypted to prevent "playback" attacks. All passwords, algorithms, keys, certificates, codes, or other schemes used for authentication shall be stored in a manner that prevents unauthorized access.

5.2 Access Control

Access controls restrict access to objects such as files, directories, and devices based upon users' identities or groups and protect against unauthorized disclosure, modification, or destruction of the data.

Automated systems are vulnerable to the fraudulent or malicious activities of individuals who have the authority or capability to access information not required to perform their job-related duties. Access control policy is designed to reduce the risk of an individual's engaging in fraudulent or malicious behavior while acting alone.. The Principle of Least Privilege states that

users should only be able to access the system resources needed to fulfill their job responsibilities. This principle should be considered when granting access.

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

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

- **Initial User Access**

Users who need access to DHS systems and networks must have completed a background investigation prior to being granted access. User access will vary depending on the user's position. The user's supervisor or Project Manager must also determine the systems the user needs to access and the levels of access the user requires. The System Owner must approve user access privileges.

- **Review of Access Privileges**

The data a user needs to access will change over time. Therefore, supervisors have the responsibility to ensure that access control lists are current and up-to-date. This requirement also applies to contractors and other non-DHS personnel with access to any DHS systems. ISSOs have an oversight responsibility to ensure this is being accomplished. These actions are reviewed as part of the Security Authorization Process process and during annual self-assessments.

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

- **Terminated and Departing Employees**

System and local area network (LAN) administrators and ISSOs must ensure that all departing employees have their access privileges terminated immediately. No former employee should have the ability to access system resources after their term of employment has ended. Procedures vary depending on whether the separation is voluntary or involuntary. Termination of access privileges also applies to employees whose job functions have changed such that they no longer require access to the level to which they were previously granted. See Section 4.1.6, Separation from Duty, for additional guidance.

- **Secure Remote Access**

Hardware security tokens, such as cryptographic smartcards, can be issued to DHS employees and contractors who have a valid need to remotely access DHS systems and data.

- **Access to Controlled Data**

Systems that store or process information requiring special controls (e.g., categories of Controlled Unclassified Information [CUI] such as Protected Critical Infrastructure Information [PCII]) must take measures to ensure that only authorized users have access to that information, regardless of whether the system utilizes dedicated assets, shared infrastructures, or virtualized or cloud technologies. Such measures must include:

- Clearly preserving the identification and access requirements of the controlled data by using data labels or dedicated storage containers
- Limiting system access to users with the appropriate credentials needed for access to the CUI or, alternatively, using internal enforcement mechanisms to ensure that only authorized users are allowed access to the controlled data
- Applying data-at-rest protections, such as dedicated protected storage or data encryption, to ensure that the data cannot be compromised by bypassing the system's enforcement mechanisms; cryptographic separation and protection is preferred, as it provides more robust protection against compromise

Users are responsible for protecting all DHS information to which they have access.

Policy ID	DHS Policy Statements	Relevant Controls
5.2.a	Components shall implement access control policy and procedures that provide protection from unauthorized alteration, loss, unavailability, or disclosure of information.	AC-1
5.2.b	Access control shall follow the principles of least privilege and separation of duties and shall require users to use unique identifiers. <i>Social Security Numbers shall not be used as login IDs.</i>	AC-5 AC-6
5.2.c	Users shall not provide their passwords to anyone, including system administrators.	IA-5
5.2.d	Emergency and temporary access authorization shall be strictly controlled and shall be approved by the Component Chief Information Security Officer (CISO) or Information Systems Security Manager (ISSM) or his/her designee prior to being granted.	AC-2
5.2.e	System Owners shall ensure that users are assigned unique account identifiers.	IA-4
5.2.f	DHS systems with a Federal Information Processing Standard (FIPS) 199 confidentiality categorization of high shall limit the number of concurrent sessions for any user to one (1) unless strong authentication is used.	AC-10

Policy ID	DHS Policy Statements	Relevant Controls
5.2.g	Components and Programs shall ensure that all data-at-rest, particularly in cloud or other virtual environments, preserves its identification and access requirements (anyone with access to data storage containing more than one type of information must have specific access authorization for every type of data in the data storage).	---

Access control responsibilities are provided in the following table.

Access Control Responsibilities
<p>Component CISOs/ISSMs</p> <p>Establish and enforce access control policy</p> <p>Provide technical expertise and evaluate the effectiveness of access control approaches</p> <p>Security Control Assessors</p> <p>Conduct assessments to verify that adequate access controls are in place</p> <p>System/Network Administrators</p> <p>Ensure that access controls are in place and functioning as intended</p> <p>Ensure that access controls provide the security features outlined in this document</p> <p>Ensure that systems prevent users from having multiple concurrent active sessions for one identification unless the AO has granted authority based upon operational business needs</p> <p>ISSOs</p> <p>Ensure that access controls are in place and functioning as intended</p> <p>Ensure that access controls provide the security features outlined in this document</p>

5.2.1 Automatic Account Lockout

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

Policy ID	DHS Policy Statements	Relevant Controls
5.2.1.a	Components shall configure accounts to automatically lock a user's <i>account</i> after three consecutive failed logon attempts.	AC-7
5.2.1.b	The automatic lockout period for accounts locked due to failed login attempts shall be set for twenty (20) minutes.	AC-7

Policy ID	DHS Policy Statements	Relevant Controls
5.2.1.c	Components shall establish a process for manually unlocking accounts prior to the expiration of the twenty (20) minute period, after sufficient user identification is established. This may be accomplished through the help desk.	AC-7

Automatic account lockout responsibilities are provided in the following table.

Automatic Account Lockout Responsibilities
<p>DHS CISO Establishes and enforces automatic account lockout policies</p> <p>System/Network Administrators Ensure that systems are configured to lock a user's account for 20 minutes after 3 unsuccessful logon attempts during a 24 hour time period</p> <p>ISSOs Ensure that systems are configured to lock a user's account for 20 minutes after 3 unsuccessful logon attempts</p>

5.2.2 Automatic Session Termination

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

Policy ID	DHS Policy Statements	Relevant Controls
5.2.2.a	Components shall configure networked applications or systems to automatically lock any user session in accordance with the appropriate configuration guide. In the absence of configuration guidance, the session shall lock following twenty (20) minutes of inactivity.	AC-11
5.2.2.b	Locked sessions shall remain locked until the user re-authenticates.	AC-11
5.2.2.c	Sessions shall automatically be terminated after sixty (60) minutes of inactivity.	SC-10

Automatic session lockout responsibilities are provided in the following table.

Automatic Session Lockout Responsibilities
<p>DHS CISO Establishes and enforces automatic session lockout policies</p> <p>System/Network Administrators Ensure that systems are configured to terminate any user session that has remained idle for 20 minutes</p> <p>ISSOs Ensure that systems are configured to terminate any user session that has remained idle for 20 minutes</p>

5.2.3 Warning Banner

The DHS CISO stipulates that a warning banner statement be displayed on all DHS systems during logon. The most current language can be found on the [DHS CISO](#) Web page.

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

The use of the warning banner serves as a reminder to all users that the computers they are accessing are Government computers.

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

Warning banner responsibilities are provided in the following table.

Warning Banner Responsibilities
<p>DHS CISO Establishes and enforces the use of appropriate standard Warning Banner for all DHS systems</p> <p>System/Network Administrators Ensure that DHS systems under their control are configured to display the approved DHS Warning Banner</p> <p>ISSOs</p>

Warning Banner Responsibilities

Ensure that all DHS systems under their control are configured to display the approved DHS Warning Banner

5.3 Auditing

Auditing is a fundamental security principle that provides the ability to track the activities of a user who is accessing an automated system. Trails maintained by auditing tools are an effective method of enforcing this principle. Audit trails maintain a record of system, application, and user activity.

With the use of appropriate tools and procedures, auditing can further progress toward several security-related objectives including:

- Individual accountability
- Intrusion detection
- Problem identification
- Capability to reconstruct events

Audit trails can track the identity of each subject attempting to access a system, the time and date of access, and the time of log off. Audit trails can also capture all activities performed during a session and can specifically identify those activities that have the potential to modify, bypass, or negate the system's security safeguards. The auditing technique used must be able to support after-the-fact investigations of how, when, and why normal operations ceased.

Audit trail records must be maintained online for at least 90 days to allow rapid access to recent information. Audit trails should be preserved for a period of seven years as part of record management for each system to allow audit information to be placed online for analysis with reasonable ease. Preservation of the audit information should be part of contingency and business continuity plans, so that events preceding a disaster or interruption of service can be reconstructed.

To be effective, audit trails must be periodically reviewed and analyzed. The capability to review the information captured by the auditing process is of paramount importance. In many cases, it is only through the review process that incidents of unauthorized access, modification, or destruction are uncovered. Audit trails need to be secured to prevent tampering and they must be backed up regularly.

Policy ID	DHS Policy Statements	Relevant Controls
5.3.a	<p>Audit records shall be sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. Audit records shall be reviewed as specified in the SP. The audit record shall contain at least the following information:</p> <ul style="list-style-type: none"> • Identity of each user and device accessing or attempting to access the system • Time and date of the access and the logoff • Activities that might modify, bypass, or negate information security safeguards • Security-relevant actions associated with processing • All activities performed using an administrator’s identity 	AU-3
5.3.b	<p>Audit records for financial systems or for systems hosting or processing Personally Identifiable Information (PII) shall be reviewed each month. Unusual activity or unexplained access attempts shall be reported to the System Owner and Component CISO/ISSM.</p>	AU-6
5.3.c	<p>Components shall ensure that their audit records and audit logs are protected from unauthorized access, modification, or destruction.</p>	AU-9
5.3.d	<p>Components shall ensure that audit logs are recorded and retained in accordance with the Component’s Record Schedule or with the DHS Records Schedule. At a minimum audit trail records shall be maintained online for at least ninety (90) days. Audit trail records shall be preserved for a period of seven (7) years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease.</p>	AU-11
5.3.e	<p>Components shall evaluate the system risks associated with extracts of PII from databases. If the risk is determined to be sufficiently high, a procedure shall be developed for logging computer-readable data extracts. If logging these extracts is not possible, this determination shall be documented, and compensating controls identified in the SP.</p>	AU-1, AU-2, AU-3, PM-9
5.3.f	<p>Component Security Operations Centers (SOC) shall implement both general and threat-specific logging.</p>	AU-1

Auditing responsibilities are provided in the following table.

Auditing Responsibilities
Component CISOs/ISSMs

Auditing Responsibilities

Ensure that all DHS systems maintain audit records sufficient to reconstruct security related events

Evaluate auditing requirements at the Component level

Budget for and select appropriate auditing tools

Establish policy for retention of audit logs

Ensure auditing is performed independently of system/network administration

System Owners

Ensure adequate resources are budgeted for implementing and maintaining an effective auditing capability

Work with managers to identify critical functions to be subjected to auditing and keep apprised of audit findings.

Ensure auditing is performed independently of system/network administration

System/Network Administrators

Maintain an audit record sufficient to reconstruct security related events

Ensure that each audit record includes:

- The identity of each person and device accessing or attempting to access the system.
- The time and date of the access or attempt and when the user logged off
- Activities performed using an administrator's identification
- Activities that could modify, bypass, or negate the system security
- Sufficient detail to facilitate reconstruction if compromise or malfunction occurs
- Security related actions associated with processing

Protect audit records against unauthorized access, modification, or destruction

Retain audit records for a minimum of ninety (90) days or in accordance with the Security Plan and ensure that audit records are regularly backed up

ISSOs

Ensure that the SP addresses accountability and auditing

Ensure that the risk analysis documents the rationale and justification for any DHS system that does not implement an auditing capability

Ensure that audit records include all required elements

Review audit records at least weekly, or in accordance with the SP

Ensure that audit collection and review procedures contain provisions for adequate separation of duties
Report security related events to the Component's Security Operations Center (SOC)

5.4 Network and Communications Security

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

5.4.1 Remote Access and Dial-In

Remote access technology allows trusted employees to access DHS networks by dialing in via modem or accessing the DHS network via the Internet. This allows mobile employees to stay in touch with the home office while traveling. There are significant security risks, however, associated with remote access and dial-in capabilities. Proper procedures can help mitigate these risks. .

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

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

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

Remote access solutions that do not comply with the requirements of FIPS 140-2 are not authorized.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.1.a	Data communication connections via modem shall be limited and shall be tightly controlled, as such connections can be used to circumvent security controls intended to protect DHS networks. Data communication connections are not allowed unless they have been authorized by the Component CISO/ISSM. Approved remote access to DHS networks shall only be accomplished through equipment specifically approved for that purpose. Tethering with wireless PEDs is prohibited unless approved by the appropriate AO.	AC-17
5.4.1.b	Components shall centrally manage all remote access and dial-in connections to their systems and shall ensure that remote access and approved dial-in capabilities provide strong two-factor authentication, audit capabilities, and protection for sensitive information throughout transmission. DHS has an immediate goal that remote access shall only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. Any two-factor authentication shall be based on Department-controlled certificates or hardware tokens issued directly to each	AC-17, AU-2 SC-8, SC-9

Policy ID	DHS Policy Statements	Relevant Controls
	authorized user. Remote access solutions shall comply with the encryption requirements of FIPS 140-2, <i>Security Requirements for Cryptographic Modules</i> . See Section 3.14 of this Policy Directive, “Privacy and Data Security” for additional requirements involving remote access of PII.	
5.4.1.c	Remote access of PII shall comply with all DHS requirements for sensitive systems, including strong authentication. Strong authentication shall be accomplished by means of virtual private network (VPN) or equivalent encryption and two-factor authentication. The Risk Assessment and Security Plan (SP) shall document any remote access of PII, and the remote access shall be approved by the AO prior to implementation.	AC-4, AC-17, AU-2 SC-7, SC-8, SC-9
5.4.1.d	Remote access of PII shall not permit the download and remote storage of information unless the requirements for the use of removable media with sensitive information have been addressed. All downloads shall follow the concept of least privilege and shall be documented with the SP.	---

Remote access and dial-in responsibilities are provided in the following table.

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

5.4.2 Network Security Monitoring

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

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

Policy ID	DHS Policy Statements	Relevant Controls
5.4.2.a	Components shall provide continuous monitoring of their networks for security events, or outsource this requirement to the DHS Security Operations Center (SOC). Monitoring includes interception and disclosure as to the extent necessary for rendering service or to protect Department or Component rights or property. Here <i>rights</i> refers to ownership or entitlements or to property or information as in intellectual property. Service observation or random monitoring shall not be used except for mechanical or service quality control checks in accordance with the Electronic Communications Privacy Act.	SI-4
5.4.2.b	The DHS SOC shall administer and monitor DHS intrusion detection system (IDS) sensors and security devices.	SI-4
5.4.2.c	Component SOCs shall administer and monitor Component IDS sensors and security devices.	SI-4

Network security monitoring responsibilities are provided in the following table.

Network Security Monitoring Responsibilities
<p>Component CISOs/ISSMs</p> <p>Establish Component policy and implement and manage a viable intrusion detection program within their Component</p> <p>Provide guidance, as needed, when responding to intrusion alerts from the DHS or Component SOC</p>
<p>DHS and Component SOC</p> <p>Monitor DHS systems and networks using various network security technologies</p> <p>Initiate computer security incident procedures when incidents are discovered</p>
<p>ISSOs/System Administrators</p> <p>Respond to intrusion alerts when notified by SOCs</p> <p>Participate in SOC-led incident response investigations</p> <p>Evaluate the impact of the event on the system</p> <p>Implement necessary corrective actions</p>

5.4.2.1 What Is Intrusion Detection?

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

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

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

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

5.4.2.2 Methods and Techniques

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

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

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

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

5.4.2.3 Monitoring

The DHS SOC shall be responsible for monitoring of DHS systems and networks. Upon receipt of an alarm, operators shall investigate to determine the validity of the alarm. Once validity is

confirmed, the operator shall notify the ISSO and/or the system administrator for corrective action. If the problem is deemed critical, senior management shall be notified and shall be involved in determining the appropriate course of action.

5.4.3 Network Connectivity

A system interconnection is the direct connection of two or more information systems for the purpose of sharing data and other information resources by passing data between each other via a direct system-to-system interface without human intervention. Any physical connection that allows other systems to share data (pass thru) also constitutes an interconnection, even if the two systems connected do not share data between them. System interconnections do not include instances of a user logging on to add or retrieve data, nor users accessing Web-enabled applications through a browser.

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

Policy ID	DHS Policy Statements	Relevant Controls
5.4.3.a	Components shall ensure that appropriate identification and authentication controls, audit logging, and access controls are implemented on every network element.	AC-1, AC-2, AU-1, AU-2, IA-1, IA-2
5.4.3.b	Interconnections between DHS and non-DHS systems shall be established only through controlled interfaces and by approved service providers. The controlled interfaces shall be authorized at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memorandums of understanding, service level agreements or interconnection security agreements.	CA-3
5.4.3.c	Components shall document all interconnections to the DHS OneNet with an Interconnection Security Agreement (ISA), signed by the OneNet AO and by each applicable AO. Additional information regarding ISAs is published in Attachment N, <i>Preparation of Interconnection Security Agreements</i> , to this Handbook.	CA-3
5.4.3.d	ISAs shall be reissued every three (3) years or whenever any significant changes have been made to any of the interconnected systems.	CA-3
5.4.3.e	ISAs shall be reviewed and updated as needed as a part of the annual Federal Information Security Management Act (FISMA) self-assessment.	CA-3

Policy ID	DHS Policy Statements	Relevant Controls
5.4.3.f	Components may complete a master Interconnection Security Agreement (ISA) that includes all transitioning systems as part of their initial OneNet transition. After transition, each additional system or General Support System (GSS) shall be required to have a separate ISA. Interconnections between DHS Components (not including DHS OneNet) shall require an ISA whenever there is a difference in the security categorizations for confidentiality, integrity, and availability between the systems or when the systems do not share the same security policies. (In this context, <i>security policies</i> refers to the set of rules that controls a system's working environment, and not to DHS information security policy). ISAs shall be signed by the appropriate AO.	---
5.4.3.g	Components shall document interconnections between their own and external (non-DHS) networks with an ISA for each connection.	CA-3
5.4.3.h	The DHS Chief Information Officer (CIO) shall approve all interconnections between DHS enterprise-level information systems and non-DHS information systems. The DHS CIO shall ensure that connections with other Federal Government agencies are properly documented. A single ISA may be used for multiple connections provided that the security authorization is the same for all connections covered by that ISA.	CA-3
5.4.3.i	The Department and Components shall implement Trust Zones by means of Policy Enforcement Points (PEP), as defined in the DHS Security Architecture.	SC-7
5.4.3.j	DHS OneNet shall provide secure Name/Address resolution service. Domain Name System Security Extensions (DNSSEC) has been designated as the DHS service solution.	SC-20, SC-21, SC-22
5.4.3.k	All DHS systems connected to OneNet and operating at moderate or high level shall utilize secure Name/Address resolution service provided by DHS OneNet.	SC-20, SC-21, SC-22
5.4.3.l	The appropriate CCB shall ensure that documentation associated with an approved change to an information system is updated to reflect the appropriate baseline. DHS systems that interface with OneNet shall also be subject to the OneNet CCB.	CM-3
5.4.3.m	Interconnections between two authorized DHS systems do not require an ISA if the interface characteristics, security requirements, nature of information communicated and monitoring procedures for verifying enforcement of security requirements are accounted for in the SPs or are described in another formal document, such as a Service Level Agreement (SLA) or contract, and the risks have been assessed and accepted by all involved AOs.	CA-3
5.4.3.n	Granting the ability to log into one DHS system through another DHS system	---

Policy ID	DHS Policy Statements	Relevant Controls
	(such as through OneNet trust) does not require an ISA, when the requirements from Section 5.4.3.m are met.	

Network connectivity responsibilities are provided in the following table.

Network Connectivity Responsibilities
<p>Component CISOs/ISSMs</p> <p>Provide guidance and enforce management, operational, and technical controls that apply to network and system security configuration and monitoring</p> <p>Evaluate the risks associated with external connections</p> <p>Review programs/systems periodically to ascertain if changes have occurred that could adversely affect security</p> <p>AO</p> <p>Review, approve, and sign the ISA</p> <p>Ensure that ISAs are reissued every three years or whenever significant changes are made to any of the interconnected systems</p> <p>System Owners</p> <p>Establish the requirement for the external connection and assess the associated risks</p> <p>Network Administrators</p> <p>Ensure technical controls governing use of the external connection remain in place and function properly</p> <p>Assist in development of the ISA</p> <p>ISSOs</p> <p>Coordinate with the external agency in development of the ISA</p> <p>Assist in preparation of the ISA and ensure all external connections are documented in the SP, Risk Assessment, and security operating procedures</p> <p>Review ISAs as a part of the annual FISMA self-assessment</p> <p>Monitor compliance</p> <p>Users</p> <p>When connecting to DHS networks, ensure the equipment used to access the networks is protected from viruses and other malicious code and the protection software is kept current</p>

5.4.3.1 Interconnection Security Agreements

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

An ISA is required whenever the security policies of the interconnected systems are not identical or the systems are not administered by the same entity or AO. The ISA documents the security protections on the interconnected systems to ensure that only acceptable transactions are permitted. Component personnel must review ISAs as part of the annual FISMA self-assessment. ISAs must be reissued every three (3) years or whenever significant changes have been made to any of the interconnected systems.

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

An ISA should contain the following:

- Purpose – This section should explain the rationale for the interconnection and contain a one- or two-paragraph statement that justifies the need to interconnect the two systems.
- Interconnection Statement of Requirements – This section documents the formal requirement for connecting the two systems. The following items should be addressed in this section:
 - The names of the systems being interconnected
 - The requirement for the interconnection, including the benefits derived
 - The type of connection (Frame Relay, T1, etc.)
 - Physical location of connection equipment, including addresses and room numbers
 - Primary Points of Contact (POC) for both systems
 - The agency name(s) or organization that initiated the requirement.
- System Security Considerations – This section documents the security features in place to protect the confidentiality, integrity, and availability of the data and the systems being interconnected. This includes such aspects as incident reporting and personnel clearances. Technical representatives from each organization need to discuss the contents of this section and come to a mutual agreement as to which items should be included.

- Topological Drawing – Each ISA must include a topological drawing depicting the end-to-end interconnectivity in a clear and readable manner. The drawing should include:
 - * All data communications paths (not program system paths), circuits, etc., used for the interconnection beginning with the DHS-owned system(s) and including all interconnected systems to the non-DHS end-point
 - * The logical location of all elements (mainframe computers, host processors, hubs, firewalls, encryption devices, routers, frame relay devices, secure frame units [SFU], communications service units [CSU], data service units [DSU], and customer personal computers).
- Signatures and Comments – Each ISA must be signed by the AO of each interconnecting system or organization, or by the official designated by the AO to have signatory authority for ISAs. This section acknowledges that the ISA is subject to change, will be reviewed annually, and will be modified as circumstances warrant. This section must include a statement that the ISA may not be unilaterally modified and that any changes must be reviewed and jointly agreed upon by the AOs of the interconnected systems. Others in the organization, however, should have the opportunity to review changes.

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

5.4.3.2 Trust Zones

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

DHS Trust Zones have the following characteristics:

- The Trust Zone must be set of networked hosts protected from unconstrained access by one or more security perimeter devices
- There must be a basis for placement and configuration of firewalls, Virtual VPNs, and remote access protection devices
- The Trust Zone may consist of a single host, one or more LANs at a site, or a group of networks connected via a network provider or backbone
- OneNet provides a layer of trust by means of sub-netting, firewalls, and other policy enforcement mechanisms
- Network Admission Control permits dynamic assignment of information systems and users to basic Trust Zones. Medium and High assurance models are another mechanism that permits assignment to Trust Zones

5.4.4 Firewalls and Policy Enforcement Points

Policy Enforcement Points (PEP) separate Trust Zones as defined in the DHS Security Architecture. Boundary protection between DHS and external networks is implemented by firewalls at the Trusted Internet Connections (TIC) and other approved direct system interconnections. DHS TICs are provided by OneNet and monitored by the DHS SOC. Component SOCs may protect DHS-internal boundaries across Trust Zones.

Within DHS, boundary protection of information system resources is accomplished by the installation and operation of firewall systems. Firewalls, when used in concert with a variety of additional security controls such as intrusion detection systems, data encryption, personnel background checks, security guards, , and physical security barriers, provide an added level of assurance that unauthorized personnel will be unable to access the Department's automated systems.

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

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

Policy ID	DHS Policy Statements	Relevant Controls
	prevent traffic as directed by the DHS CIO.	
5.4.4.j	The DHS SOC shall oversee all enterprise PEPs.	---

Responsibility for deployment and management of firewalls are included in the following table.

Firewall Responsibilities
<p>Component CISOs/ISSMs Develop procedures and schedules for deploying firewall systems</p> <p>ISSOs and ADP Support Personnel Assist Component teams in the installation and configuration of firewall systems</p> <p>Site Managers Ensure that the firewall installation team receives necessary support during and after installation</p> <p>SOCs Manage firewalls in accordance with DHS firewall policy Maintain change control over firewalls and maintain proper firewall configuration Evaluate, process, and approve changes to firewall configuration</p>

5.4.4.1 Firewall Basics

A firewall is a system or group of systems that enforce an access control policy between two networks. The actual means by which this is accomplished vary widely. Firewalls can authenticate the source and destination of a given data path provide network address translation (NAT) and port address translation (PAT) and log all traffic passing through them. Logging is either done on the machine on which the firewall software runs on, or is logged to a separate machine for audit and intrusion forensic analysis.

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

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

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

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

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

5.4.4.2 Firewall Deployment

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

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

5.4.4.3 Firewall Management

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

5.4.5 Internet Security

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

Sound network security practice dictates that all network connections be identified and that the threats and vulnerabilities associated with these connections be analyzed. The guidance provided in Section 5.4.3, *Network Connectivity*, specifically that with regard to ISAs, and in Attachment N to this Handbook, *Preparation of Interconnection Security Agreements*, also applies to connections to the Internet and extranets. An *extranet* is a private network encompassing that portion of an organization's intranet that it chooses to securely share, via the Internet and the public telecommunication system, with external entities, which may include suppliers, vendors, and customers. An extranet requires security and privacy and may involve firewalls, digital certificates, message encryption, and virtual private networks that can tunnel through the public network.

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

Adequate protection requires proper selection and installation of firewalls and other boundary devices, Intrusion Detection Systems, and ancillary encryption or filtering devices. These devices must be assessed and authorized prior to their use on DHS networks. Implementation guidance for firewalls is discussed in Section 5.4.4 of this Handbook, "Firewalls." Intrusion Detection Systems are covered in Section 5.4.2; encryption is addressed in Section 5.5.1. The adequacy of all of these must be monitored and reviewed as part of periodic information security assessments.

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

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

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

Use of the following is expressly prohibited:

- Telnet

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

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

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

Implementation guidance for securing dial-up connections is addressed in Section 5.4.1, Remote Access and Dial-In. Dial-in connections must be strictly controlled, to the extent they can even be justified.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.5.a	Any direct connection of OneNet, DHS networks, or DHS mission systems to the Internet or to extranets shall occur through DHS TIC PEPs. The PSTN shall not be connected to OneNet at any time.	SC-7
5.4.5.b	Firewalls and PEPs shall be configured to prohibit any protocol or service that is not explicitly permitted.	CM-7, SC-7, SC-8, SC-9
5.4.5.c	Components shall ensure that all executable code, including mobile code (e.g., ActiveX, JavaScript), is reviewed and approved by the Program Manager prior to the code being allowed to execute within the DHS environment. [Note: When the technology becomes available and code can be vetted for security, the policy will be “Ensure that all approved code, including mobile code (e.g., ActiveX, JavaScript), is digitally signed by the designated DHS authority and that only signed code is allowed to execute on DHS systems.”]	SC-18
5.4.5.d	Telnet shall not be used to connect to any DHS computer. A connection protocol such as Secure Shell (SSH) that employs secure authentication (two factor, encrypted, key exchange) and is approved by the Component shall be used instead.	CM-7, SC-7, SC-8, SC-9
5.4.5.e	File Transfer Protocol (FTP) shall not be used to connect to or from any DHS computer. A connection protocol that employs secure authentication (two factor, encrypted, key exchange) and is approved by the Component shall be used instead.	CM-7, SC-7, SC-8, SC-9

Policy ID	DHS Policy Statements	Relevant Controls
5.4.5.f	Remote Desktop connections, such as Microsoft’s Remote Desktop Protocol (RDP), shall not be used to connect to or from any DHS computer without the use of an authentication method that employs secure authentication (two-factor, encrypted, key exchange).	AC-17, IA-2
5.4.5.g	In order to ensure the security and availability of DHS information and information systems, the DHS CIO or DHS CISO may direct that specific Internet websites or categories be blocked at the DHS TICs, on advice from the United States Computer Emergency Readiness Team (US-CERT), the DHS SOC, or other reputable sources.	---

Internet security responsibilities are provided in the following table.

Internet Security Responsibilities
<p>AO</p> <p>Ensures all external network connections are protected by a firewall and possibly other boundary protection devices that have been assessed and authorized at a level commensurate with the sensitivity of the information to be protected</p> <p>Ensures dial-up connections are addressed in the Security Authorization Process documentation</p> <p>ISSOs</p> <p>Ensure all external network connections are addressed in the risk assessment and SP</p> <p>Ensure all external network connections are protected by a firewall and possibly other boundary protection devices</p> <p>Ensure all boundary protection devices are properly configured and monitored</p> <p>Ensure dial-up connections are properly configured and secure</p> <p>Network/System Administrators</p> <p>Ensure that all boundary protection devices are properly configured and monitored</p> <p>Ensure that firewall ports that allow file and printer sharing, whether through Microsoft NetBIOS, CIFS, NFS, or TCP SMB are closed</p> <p>Ensure that firewalls are configured to prohibit any protocol or service that is not explicitly permitted.</p> <p>Ensure that the following are prohibited:</p> <ul style="list-style-type: none"> – Telnet (clear text) connections – FTP unsecured (clear text) file transfers – SNMP protocols that can be used to monitor and control systems – Cross boundary routing broadcasts

Internet Security Responsibilities	
–	Address Resolution Protocol (ARP) messages
–	DNS communications across the boundary (by using split DNS with zone transfer authentication)
–	Unsecured file transfers
–	Mobile code (e.g., ActiveX, JavaScript) that has not been reviewed and digitally signed by an appropriate DHS authority
Ensure that dial-up connections are properly configured and secure	

5.4.6 Email Security

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

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

E-mail is the most commonly used application for exchanging data electronically. The email process is divided into two main elements:

- Mail servers, which deliver, forward, and store mail
- Clients, which interface with the user and allow them to read, compose, send, and store messages

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

Second only to Web servers, mail servers are the host on a network that is most often targeted by intruders. Mail servers are targeted because they communicate, to some degree, with untrusted third parties. Additionally, email has been an effective method of passing malicious code (viruses). As a result, mail servers, mail clients, and the network infrastructure that supports them must be protected. Email security issues include:

- Flaws in the email application software have been used as the means of compromising first the server and subsequently the associated network
- Denial of service (DoS) attacks may be directed to the mail server

- Sensitive information on the mail server may be read by unauthorized individuals or changed in an unauthorized manner
- Unencrypted sensitive information transmitted between a mail server and email client could be intercepted
- Information in email messages may be altered at some point between the sender and recipient
- Viruses and other types of malicious code may be distributed throughout an organization via email
- The sending of inappropriate, proprietary, or other sensitive information via email could expose an organization to legal action

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

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

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

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

The infrastructure that supports the network plays a vital role in the security of the email system. The network infrastructure is the first line of defense between the Internet and a mail server. Network design alone, however, cannot protect a mail server. The following steps need to be accomplished on a according to a regular schedule:

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

- Scan the system for vulnerabilities with a vulnerability-scanning tool

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

Policy ID	DHS Policy Statements	Relevant Controls
5.4.6.a	Components shall correctly secure, install, and configure the underlying email operating system.	---
5.4.6.b	Components shall correctly secure, install, and configure mail server software.	---
5.4.6.c	Components shall secure and filter email content.	---
5.4.6.d	Components shall deploy appropriate network protection mechanisms, such as <ul style="list-style-type: none"> - Firewalls - Routers - Switches - Intrusion detection systems 	---
5.4.6.e	Components shall secure mail clients.	---
5.4.6.f	Components shall conduct mail server administration in a secure manner. This includes: <ul style="list-style-type: none"> - Performing regular backups - Performing periodic security testing - Updating and patching software - Reviewing audit logs at least weekly 	---
5.4.6.g	The DHS email gateway Steward shall provide email monitoring for malware activity at the gateway.	SI-3
5.4.6.h	The DHS email gateway Steward shall provide email monitoring for spam at the gateway.	SI-8
5.4.6.i	Auto-forwarding or redirecting of DHS email to any address outside of the .gov or .mil domain is prohibited and shall not be used. Users may manually forward individual messages after determining that the risks or consequences are minimal.	---
5.4.6.j	All DHS email systems are required to use the common naming convention with distinguishing identifiers for military officers, contractors, foreign nationals, and U.S. Government personnel from other Departments and agencies.	---

Policy ID	DHS Policy Statements	Relevant Controls
5.4.6.k	When sending email containing any unencrypted sensitive information, particularly sensitive PII, users should use caution. When sending such information outside the dhs.gov domain, users shall ensure that the information is encrypted.	

Note: Due to the significant risk associated with HTML email, DHS is considering following the lead of the Department of Defense (DOD) and moving to text based email.

Email security responsibilities are provided in the following table.

Email Responsibilities
<p>DHS CISO Establishes Department-wide policy to secure email systems</p> <p>Component CISOs/ISSMs Advise the DHS CISO on methods for securing Department email systems Enforce Department email security policies</p> <p>Security Control Assessors Conduct assessments to determine that adequate security controls are in place for email systems</p> <p>AOs Ensure that adequate email security controls are in place prior to authorization of the system</p> <p>System/Network Administrators Ensure that email security controls are in place and functioning as intended Ensure that email security controls provide the security features named in this document Test and apply patches in a timely manner Remove or disable unneeded services and applications on email servers Configure user authentication for email systems Review and analyze log files. Back up data as required by the Security Plan Protect email systems against malicious code Deploy the following network protection mechanisms:</p> <ul style="list-style-type: none"> – Firewalls – Routers – Switches

Email Responsibilities
<p>– Intrusion detection systems</p> <p>ISSOs</p> <p>Schedule semiannual or quarterly appointments with the SOC or IV&V team to scan the email system with a vulnerability assessment tool</p> <p>Ensure that email system security controls are in place and functioning as intended</p> <p>Ensure that email system security controls provide the security features named in this document and in the SP</p> <p>Ensure that a tested Contingency Plan is in place</p>

5.4.7 Personal Email Accounts

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

Sending email to a personal account has the following vulnerabilities:

- DHS does not authorize the use of personally owned computers within DHS; they are not likely to have the appropriate encryption software installed, thus information is sent in “clear text”
- The route that the email travels cannot be predicted
- Untrusted persons at ISP sites may read sensitive information
- Email travels over unprotected communication links that can be “sniffed” in transit, exposing messages to being read by unauthorized persons
- Web browsers are often used to access private email accounts and such access is inherently not secure
- Malware (which could exist on the employee’s personal computer) can send copies of existing emails or other text on a victim’s computer to unknown individuals
- Instant Messaging channels are a frequent source of malware and of mechanisms for attacks on personal computers
- So-called “spyware” programs transmit information from personal computers to unknown sites. Some programs (both freeware and commercial) install these programs to harvest marketing information and other information from a user’s computer.

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

Policy ID	DHS Policy Statements	Relevant Controls
5.4.7.a	The use of Internet Webmail (Gmail, Yahoo, AOL) or other personal email accounts is not authorized over DHS furnished equipment or network connections.	---

Personal email responsibilities are provided in the following table.

Personal Email Responsibilities
<p>DHS CISO Establishes DHS policy concerning the transmittal of sensitive information Evaluates the risks associated with the transmittal of sensitive information</p> <p>Component CISOs/ISSMs Evaluate the risks and recommend solutions to counter the risk of transmitting sensitive information</p> <p>System Owners and Supervisors Enforce DHS policy prohibiting the transmittal of sensitive information to personal email accounts</p> <p>System Administrators Ensure that technical controls are in place and properly functioning to prohibit and/or deter the transmission of sensitive DHS information to personal email accounts</p> <p>ISSOs Ensure that technical controls are in place and properly functioning to prohibit and/or deter the transmission of sensitive DHS information to personal email accounts Monitor compliance with DHS policy compliance</p> <p>Users Comply with DHS policy prohibiting the transmission of sensitive information to personal email accounts</p>

5.4.8 Testing and Vulnerability Management

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

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

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

The DHS ISVM Program, managed through the SOC, provides Component CISOs/ISSMs and operational support personnel (e.g., ISSOs, System Administrators) with bulletins, alerts, and technical advisories related to emerging vulnerabilities and threats. The ISVM is modeled on the Department of Defense Information Assurance Vulnerability Assessment (IAVA) program but generally does not prescribe mitigation options nor centrally manage software patching. The following ISVM tools are available to support the Component CISO/ISSM:

- DHS Top 20 Critical Vulnerabilities List
- DHS Vulnerability Assessment Team (VAT) – Red Team for Components without internal capabilities and for independent verification as necessary
- DHS Vulnerability Assessment Request Form (see Appendix O2 of DHS 4300A Attachment O to this handbook)
- Negotiated pricing for vulnerability assessment tools (pending)

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

Policy ID	DHS Policy Statements	Relevant Controls
5.4.8.a	Components shall conduct vulnerability assessments and/or testing to identify security vulnerabilities on information systems containing sensitive information annually or whenever significant changes are made to the information systems. This shall include scanning for unauthorized wireless devices on the network. Evidence that annual assessments have been conducted shall be included in SARs and with annual security control assessments.	---
5.4.8.b	Component CISOs/ISSMs shall approve and manage all activities relating to requests for Vulnerability Assessment Team (VAT) assistance in support of incidents, internal and external assessments, and on-going SLC support.	---
5.4.8.c	Component CISOs/ISSMs or their designated representatives shall acknowledge receipt of ISVM messages.	SI-5
5.4.8.d	Components shall report compliance with the ISVM message within the specified time. Components not able to do so shall submit documentation of a waiver request via the DHS SOC Online Portal (https://soconline.dhs.gov).	SI-5

Policy ID	DHS Policy Statements	Relevant Controls
5.4.8.e	When vulnerability assessment responsibilities encompass more than one Component, Component CISOs/ISSMs shall coordinate with the relevant Component SOC and the DHS SOC.	RA-3
5.4.8.f	The DHS SOC shall be notified before any ISVM scans are run.	RA-5
5.4.8.g	System Owners shall report the security alert and advisory status of the information system to the AO, Component CISO/ISSM, and DHS CISO upon request and on a periodic basis.	SI-5

Testing and vulnerability assessment responsibilities are provided in the following table.

Testing and Vulnerability Assessment Responsibilities
<p>Component CISOs/ISSMs</p> <p>Develop and follow POA&M procedures for implementing vulnerability assessments on sensitive systems</p> <p>Approve and manage all activities relating to requests for VAT assistance in support of incidents, internal and external assessments, and on-going Systems Engineering Life Cycle (SELC) support</p> <p>Ensure coordination among the DHS SOC, the Component SOC, and the ISVM Program when vulnerability assessments cross multiple Component responsibilities</p> <p>ISSOs and Information System Support Personnel</p> <p>Support SOC vulnerability assessments</p>

5.4.8.1 Vulnerability Scanning

Vulnerability scanning is the process of identifying known vulnerabilities of information systems operating on a network in order to determine if a system can be compromised. Vulnerability scanning often employs software that contains databases of known flaws, and tests systems for the occurrence of these flaws.

Vulnerability scanning typically refers to system audits on internal networks that are not connected to the Internet, as well as to systems that are visible on the Internet. The purpose of vulnerability scanning is to identify weaknesses in a system (or in system security procedures, hardware design, internal controls, etc.) that could be exploited to gain unauthorized access or to affect the systems' availability or data integrity.

Staff members performing this type of testing shall be cleared to the levels commensurate with that of the system being tested.

5.4.8.2 Expanded Vulnerability Scanning

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

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

5.4.8.3 Gap Analysis

Gap analysis determines the variance between requirements current capabilities. It requires that the testers have access to internal information such as security policy and procedure documents and specific networks or systems that should be assessed. Internal staff or, preferably, third parties can perform gap analyses.

5.4.8.4 Penetration Testing

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

5.4.8.5 Scope of Vulnerability Assessments

All equipment attached to the DHS information system infrastructure is subject to security vulnerability scanning. In today’s changing environment, vulnerable and/or unprotected systems can easily be overlooked. Systems that are not properly managed can become potential threats to the health of the DHS infrastructure.

Proactive security scanning allows for a meaningful assessment of system security against known risks, provides a roadmap of effective countermeasures for improving security, leads to faster

detection of vulnerabilities, and reduces damage to breached systems. Proactive scanning can also identify authorized and unauthorized devices on the internal network, such as unauthorized wireless access points, modems or high-speed links installed by employees for their personal convenience.

Any system identified in conjunction with a security incident shall be subject to a comprehensive security scan. Random network scans shall not be advertised, but the DHS SOC shall be informed prior to conducting any scans.

Network and host scans shall be conducted by authorized DHS personnel using pre-designated scanning machines in order to be easily recognizable as benign activity in system log files. Because vulnerability scanning can be resource intensive, routine scanning is to be done during periods of low network activity when feasible.

5.4.9 Peer-to-Peer Technology

Peer-to-peer technology refers to applications that allow individual PCs to act as servers to other individual PCs. This technology was made popular by music file-swapping services (e.g., Napster, Kazza, etc.). Peer-to-peer technology allows users to share files with each other through a network of computers that use the same peer-to-peer client. Each computer has the ability to act as both a server, by hosting files for others to download, and a client by searching other computers for files the client wants to access.

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

Peer-to-peer applications circumvent most enterprise security systems. This provides malicious users easy access, allowing them to install malware, identify IP addresses or user names, launch denial of service attacks, gain control of network resources, or access sensitive information.

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

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

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

[For additional information on inappropriate use of DHS resources, see Section 3.12, “Information Technology Security Policy Violation and Disciplinary Action;” Section 4.8.3, “Personally Owned Equipment and Software;” Section 4.8.5, “Personal Use of Government Office Equipment and Department of Homeland Security Information Technology Systems/Computers;” and Section 4.9, “Security Incidents and Incident Response and Reporting.”]

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

Peer-to-peer responsibilities are provided in the following table.

Peer-to-Peer Technology Responsibilities
<p>DHS CIO, CISO Establish DHS policy regarding the unauthorized use of information system technology and software</p> <p>Component CISOs/ISSMs Ensure that controls, including awareness training, are in place to minimize or prevent unauthorized use of unauthorized information system technology and software</p> <p>Supervisors Enforce unauthorized use policies including remedial training and other sanctions Promptly report unauthorized use of information system technology in accordance with DHS Computer Security Incident reporting policy (see Attachment F to this Handbook)</p> <p>ISSOs, Network/System Administrators Ensure that controls are in place including the use of monitoring and auditing to detect unauthorized use or installation of software Promptly report unauthorized use of information system technology in accordance with DHS Computer Security Incident reporting policy (Attachment F to this Handbook)</p> <p>Users Be aware of the prohibition against the use of unauthorized information system technology and software Adhere to the Unauthorized Use policies established in this section and in other references provided by DHS security officials Promptly report unauthorized use of information system technology in accordance with DHS Computer Security Incident reporting policy (Attachment F to this Handbook) Be aware of and understand the ramifications of penalties involving infractions of the rules regarding inappropriate use of Government resources</p>

5.5 Cryptography

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

This science relies on two basic components, namely an algorithm, for example Advanced Encryption Standard (AES) and a key. The algorithm is the mathematical function used for encryption or decryption, and the key is the parameter used in the transformation.

The two basic types of cryptography are: secret key systems (also called symmetric key systems) and public key systems (also called asymmetric key systems).

In secret key systems, the same key is used for both encryption and decryption; that is, all parties participating in the communication share a single key that must be securely distributed and protected.

In public key systems, each user is assigned his own pair of uniquely related keys: a private key known only to the key pair's owner, and a public key that can be made publically available. Unlike secret key systems, the only keys that need to be shared are the public keys.

The two keys are mathematically related, but the private key cannot be determined from the public key and the public key cannot be determined from the private key.

Encryption using a public key system works as follows:

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

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

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

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

5.5.1 Encryption

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

Policy ID	DHS Policy Statements	Relevant Controls
5.5.1.a	Systems requiring encryption shall comply with the following methods: <ul style="list-style-type: none"> • Products using FIPS 197 Advanced Encryption Standard (AES) algorithms with at least 256 bit encryption that have been validated under FIPS 140-2 • National Security Agency(NSA) Type 2 or Type 1 encryption – (Note: The use of triple Data Encryption Standard [3DES] and FIPS 140-1 is no longer permitted.)	IA-7, SC-13
5.5.1.b	Components shall develop and maintain encryption plans for sensitive information systems.	IA-7, SC-13
5.5.1.c	Components shall use only cryptographic modules that are FIPS 197 (AES-256) compliant and have received FIPS 140-2 validation at the level appropriate to their intended use.	IA-7, SC-13

Encryption responsibilities are provided in the following table

Encryption Responsibilities
<p>DHS CISO Develops DHS cryptography policy and approves Component encryption methodologies</p> <p>AOs Ensure that sensitive or classified encryption applications under their authority have developed encryption plans for systems prior to authorization Ensure that personnel implementing encryption requirements are technically qualified and adequately trained in encryption technologies and in the specific methodologies employed</p> <p>Component CISOs/ISSMs Ensure that DHS encryption policy is implemented and enforced Advise Project Managers on the implementation of DHS encryption standards</p> <p>ISSOs Ensure that encryption is properly implemented and configured on DHS systems Assist System Owners in identifying sensitive DHS data that requires encryption</p>

5.5.2 Public Key Infrastructure

A PKI is an architected set of systems and services that provide a foundation for enabling the use of public key cryptography. This is necessary in order to implement strong security services and to allow the use of digital signatures.

The principal components of a PKI are the public key certificates, registration authorities (RA), certification authorities (CA), directory, certificate revocation lists (CRL), and a governing certificate policy (CP).

Components that implement a PKI or CA must ensure that the CA is subordinate to the DHS Principal CA. The use of self-signed certificates has minimal security value and violates DHS policy. 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 DHS CISO.

A public key certificate is an electronic document that binds a public key to a subscriber (person, application, or device who owns the key pair). The certificate is issued and digitally signed by a trusted CA and posted to an online directory. The CA also revokes certificates whenever the binding is no longer valid or the subscriber is no longer authorized to have the certificate. Revoked certificates are published as part of the CRL. The online directory and CRL are available to the intended community.

The DHS PKI is part of a U.S. Federal PKI hierarchy. CAs in a hierarchical PKI operates under the same CP, in this case the U.S. Common Policy Framework. The U.S. Common Root CA is at the top of this hierarchy and the DHS Principal CA is subordinate. All DHS CAs must be subordinate to the DHS Principal CA.

Every CA owns a key pair and uses the private key to sign the certificates and CRLs it issues. Each CA's public key is bound to it by a public key certificate issued a CA at the next higher level of the hierarchy. The top CA is called the Root CA. The Root CA signs its own public key certificate and is the trust anchor for the entire PKI. This self-signed certificate is securely provided to all subscribers and to external relying parties who rely on certificates issued by the PKI. Certificates issued by all CAs lower in the hierarchy derive their trust from the Root CA certificate.

The RA is a service performed by highly trusted persons known as PKI registrars. PKI registrars authenticate the subscribers' identities and associated information to be included in the certificate, and when appropriate, direct the CA to issue (or reissue) a certificate. PKI registrars also interact with the CA to perform certificate lifecycle management functions such as certificate revocation.

The level of assurance is the degree to which a certificate should be trusted, and is determined by a CP that governs the operations of the CA, RA, and directory, and governs the appropriate use of the certificates and protection of private keys.

A Bridge CA provides a mechanism (cross-certification) for multiple PKIs to trust each other's certificates. The Federal PKI Policy Authority (FPKI PA) has established the Federal Bridge Certification Authority (FBCA) to enable U.S. Federal PKI, and other Government, commercial and organization PKIs to trust each other's certificates. This is accomplished through a PKI's Root CA cross certifying with the FBCA, or by another Bridge CA cross-certifying with the FBCA. In the later case, trust is extended among all of the PKIs that are cross certified with either Bridge CA.

Trust among cross-certified PKIs is based on a standard CP defined by the FPKIPA for the FBCA. This CP defines the policies that PKIs must follow in order to issue certificates at several

levels of assurance. PKIs or Bridge CAs that apply for cross certification to FBCA must operate under a CP that defines a policy that is at least equivalent to the FBCA policy. They must also demonstrate that they comply with their policy by submitting a compliance audit performed by an independent PKI auditor.

The U.S. Common Policy Root CA is cross-certified with the FBCA at high, medium hardware and medium levels of assurance. This cross-certification significantly broadens the community that can trust certificates issued by the DHS Principal CA.

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.a	<p>DHS shall implement two distinct PKIs:</p> <p>DHS FPKI: DHS shall implement a DHS Public Key Infrastructure (PKI) that is part of the Federal PKI to facilitate the use of PKI within DHS, and to facilitate the interoperable use of PKI between DHS and its external mission and business partners, such as other federal agencies; state, local and tribal governments; public and private sector entities; and U.S. citizens.</p> <p>DHS Internal Use NPE PKI: DHS shall implement a DHS Internal Use Non-Person Entity (NPE) PKI consisting of individual DHS Component PKIs used to issue certificates to the DHS Component's NPEs to support NPE-to-NPE authentication on the Component's networks, and where the certificates have no external relying parties.</p>	SC-17
5.5.2.b	<p>The DHS CISO shall be the DHS PKI Policy Authority (PKIPA) to provide PKI policy oversight for all DHS PKIs.</p> <p>DHS FPKI: A detailed description of DHS PKIPA roles and responsibilities are provided in the Registration Practice Statement for the DHS Principal Certification Authority.</p> <p>DHS Internal Use NPE PKI: A detailed description of DHS PKIPA roles and responsibilities are provided in the DHS X.509 Internal Use NPE Certificate Policy.</p>	SC-17
5.5.2.c	<p>The DHS CISO shall represent DHS on the Federal PKI Policy Authority (FPKIPA).</p>	SC-17
5.5.2.d	<p>The DHS PKIPA shall appoint a PKI Management Authority (PKIMA) to provide management and operational oversight for all DHS PKIs.</p> <p>DHS FPKI: A detailed description of DHS PKIMA roles and responsibilities are provided in the Registration Practice Statement for the DHS Principal Certification Authority.</p> <p>DHS Internal Use NPE PKI: A detailed description of DHS PKIMA roles and responsibilities are provided</p>	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
	in the DHS X.509 Internal Use NPE Certificate Policy	
5.5.2.e	<p>DHS FPKI: The DHS FPKI shall be governed by the U.S. Common Policy Framework certificate policy approved by the FPKIPA, and by the relevant portions of the Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy approved by the Department of the Treasury Policy Management Authority (PMA).</p> <p>DHS Internal Use NPE PKI: The DHS Internal Use PKI shall be governed by the DHS X.509 Internal Use NPE Certificate Policy approved by the DHS PKIPA.</p>	SC-17
5.5.2.f	<p>For the DHS FPKI: DHS shall have a single DHS Principal CA (i.e., DHS CA4) that has the U.S. Common Policy Root CA as its trust anchor. The DHS Principal CA shall be operated for DHS by the Department of Treasury under the Federal Shared Service Provider (SSP) program.</p>	SC-17
5.5.2.g	<p>DHS FPKI: The DHS Principal CA shall be the only DHS CA subordinated to the Treasury Root CA. Additional DHS CAs subordinate to the DHS Principal CA are not permitted.</p> <p>DHS Internal Use NPE PKI: A DHS Component may implement: (1) a PKI consisting of a single self-signed Internal Use NPE CA, or (2) a two-level hierarchical PKI with one Internal Use NPE Root CA and one or more Internal Use NPE CAs directly subordinated to the Internal Use NPE Root CA. The requirements and process for becoming a DHS Component Internal Use NPE Root or Subordinate CA shall be specified in the DHS X.509 Internal Use NPE Certificate Policy.</p>	SC-17
5.5.2.h	<p>DHS FPKI: The DHS Principal CA shall have a trust path resolving to the U.S. Common Policy Root CA via the Treasury Root CA. Establishing direct trust relationships with any other CAs is not permitted.</p> <p>The U.S. Common Policy Root CA is cross-certified with the Federal Bridge CA at the high, medium hardware, and medium assurance levels.</p> <p>DHS Internal Use NPE PKI: For a DHS Component with a single Internal Use NPE CA, the CA shall be self-signed and function as its own trust anchor.</p> <p>For a DHS Component with a two-level hierarchical Internal Use NPE PKI, the trust path from subordinate CAs shall resolve to the Component's Internal Use NPE Root CA.</p> <p>Establishing trust relationships with any other CAs is not permitted.</p>	SC-17
5.5.2.i	<p>DHS FPKI: The DHS Principal CA shall operate under an X.509 Certification Practice</p>	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
	<p>Statement (CPS). The CPS shall comply with the U.S. Common Policy Framework and the Treasury Certificate Policy. Since the Department of the Treasury, as the SSP for DHS, operates the DHS Principal CA, the Department of the Treasury PKI Policy Management Authority, shall approve the CPS for the DHS Principal CA.</p> <p>DHS shall operate two Registration Authorities for the DHS Principal CA. The DHS PCA Registration Authority (DHS PCA RA) shall be responsible for performing the life-cycle administration for non-PIV certificates, and the DHS PCA PIV Registration Authority (DHS PCI PIV RA) shall be responsible for performing the life-cycle administration of PIV certificates.</p> <p>The two DHS Registration Authorities for the DHS Principal CA shall operate under the Registration Practice Statement for the DHS Principal Certification Authority (RPS). The RPS shall be approved by the DHS PKIMA and the DHS PKIPA, and shall be approved for conformance to the U.S. Common Policy Framework and the Treasury Certificate Policy by the Department of the Treasury PKI Policy Management Authority.</p> <p>DHS Internal Use NPE PKI: DHS Component Internal Use NPE CAs shall operate under a Certification Practice Statement (CPS) in the form of a DHS NPE Configuration and Operation Practices Guide (COPG). The COPG shall comply with the DHS X.509 Internal Use NPE Certificate Policy. The COPG shall be approved by the DHS PKIPA.</p>	
5.5.2.j	<p>DHS FPKI: The DHS PKIMA shall ensure that the DHS PCA Registration Authority (DHS PCA RA) operates in compliance with the RPS.</p> <p>The DHS PIV Card Issuer (PCI) Organization Identity Management Official (DHS OIMO) shall ensure that the DHS PCA PIV Registration Authority (DHS PCI PIV RA) operates in compliance with the RPS.</p> <p>DHS Internal Use NPE PKI: The DHS PKIMA shall ensure that every Component Internal Use NPE CA operates in compliance with its approved DHS NPE Configuration and Operation Practices Guide (COPG).</p>	SC-17
5.5.2.k	<p>DHS FPKI: The DHS Principal CA shall undergo regular PKI compliance audits as required by the U.S. Common Policy Framework. The audit findings, report, and Plans of Action and Milestones (POA&Ms) that address deficiencies found shall be provided to the DHS PKIPA and DHS PKIMA.</p> <p>DHS Internal Use NPE PKI: Every Component Internal Use NPE CA shall undergo regular PKI compliance assessments as required by the DHS X.509 Internal Use NPE Certificate Policy. The assessment findings, report, and Plans of Action and Milestones (POA&Ms) that address deficiencies found shall be provided to the DHS PKIPA and DHS PKIMA.</p>	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.1	<p>DHS FPKI: The DHS Principal CA shall archive records as required by the U.S. Common Policy Framework, the Treasury Certificate Policy, and the DHS Principal CA CPS.</p> <p>DHS Internal Use NPE PKI: Every Component Internal Use NPE CA shall archive records as required by the DHS X.509 Internal Use NPE Certificate Policy.</p>	SC-17
5.5.2.m	<p>DHS FPKI: All operational PKI facilities shall be established in accordance with U.S. Common Policy Framework physical security requirements based on the CA's assurance level and its intended use. Location/protection of the CA shall be determined by its level of assurance. Measures taken to ensure the continuity of PKI operations shall provide at least the same level of PKI Services availability as the individual and composite availability requirements of the systems and data protected by the certificates.</p> <p>DHS Internal Use NPE PKI: All operational PKI facilities shall be established in accordance with DHS X.509 Internal Use NPE Certificate Policy physical security requirements based on the CA's assurance level and its intended use. Location/protection of the CA shall be determined by its level of assurance. Measures taken to ensure the continuity of PKI operations shall provide at least the same level of PKI Services availability as the individual and composite availability requirements of the systems and data protected by the certificates.</p>	SC-17
5.5.2.n	<p>DHS FPKI: The DHS Principal CA shall only issue certificates to internal DHS entities, e.g., Person Entities (PEs) such as employees, contractors, affiliates, roles, groups, and NPEs such as hardware devices, systems, and applications.</p> <p>External entities that require certificates to securely interact with DHS shall acquire the certificates from: (1) another Federal Agency's PKI or SSP PKI operating under the U.S. Common Policy Framework or (2) a non-Federal Agency PKI that is cross-certified with the FBCA at medium, mediumHardware, PIV-I, or high assurance level).</p> <p>DHS Internal Use NPE PKI: DHS Component Internal Use NPE CAs shall only issue certificates to the Component's internal hardware devices and systems, which are specifically permitted by the DHS X.509 Internal Use NPE Certificate Policy.</p>	SC-17
5.5.2.o	<p>DHS FPKI: Only the DHS Principal CA shall issue certificates to DHS PEs, i.e., DHS employees, contractors, affiliates, roles and group entities. Types of PE certificates that may be issued include authentication, digital signature verification and encryption certificates, including certificates for DHS HSPD-12 Personal Identity Verification (PIV) Cards, code signing and content signing, as well as all other types of certificates allowed under the U.S. Common Policy</p>	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
	<p>Only the DHS Principal CA shall issue certificates to DHS NPEs, i.e., hardware devices, systems and applications, when the following conditions apply:</p> <ul style="list-style-type: none"> • There are external relying parties for the certificates , • The certificates will be used to protect sensitive DHS data or to authenticate to operational systems containing sensitive data, and <p>The certificates are not explicitly authorized to be issued by DHS Component Internal Use NPE CAs in the DHS X.509 Internal Use NPE Certificate Policy.</p>	
5.5.2.p	<p>DHS Internal Use NPE PKI: DHS Component Internal Use NPE CAs shall only issue authentication certificates to DHS Component NPEs, i.e., hardware devices and systems, when all of the following conditions apply:</p> <ul style="list-style-type: none"> • There are no relying parties for the certificates external to the DHS Component. • The certificates will not be used to protect sensitive DHS data or to authenticate to operational systems containing sensitive data. • The certificates are explicitly authorized to be issued by DHS Component Internal Use NPE CAs in the DHS X.509 Internal Use NPE Certificate Policy. <p>A DHS Component Internal Use NPE Root CA may issue a subordination certificate to a subordinate DHS Component Internal Use NPE CA in that Component as authorized by the DHS X.509 Internal Use NPE Certificate Policy.</p>	SC-17
5.5.2.q	<p>The use by DHS of any non-DHS PKI provider for CA or PKI services is prohibited unless approved by the DHS CISO on a case-by-case basis.</p>	SC-17
5.5.2.r	<p>DHS FPKI: Only certificates that are issued by the DHS Principal CA under the U.S. Common Policy Framework at medium assurance or above shall be used to protect sensitive DHS data or to authenticate to operational systems containing sensitive data.</p> <p>Certificates issued by test, pilot, third party, self-signed or other CAs shall not be used to protect sensitive data, or to authenticate to DHS operational systems containing sensitive data.</p> <p>DHS Internal Use NPE PKI: Certificates issued by DHS Component Internal Use NPE CAs, shall not be used to encrypt sensitive data.</p>	SC-17
5.5.2.s	<p>DHS FPKI: For an external-facing DHS web server, where the browsers used by external relying parties are unable to validate DHS SSL/TLS certificates, the use of an</p>	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
	Extended Validation (EV) SSL/TLS certificate acquired from a major U.S. commercial certificate provider may be used, if approved by the DHS CISO on a case-by-case basis.	
5.5.2.t	<p>Commercial applications or appliances used by DHS that require the use of PKI certificates shall obtain those certificates from the DHS Principal CA or a DHS Component Internal Use NPE CA, as appropriate.</p> <p>Commercial applications or appliances, that require the use of a proprietary CA implemented as an internal feature, shall not be acquired or used, unless prior concurrence by the DHS PKIMA and approval by the DHS PKIPA are obtained.</p>	SC-17
5.5.2.u	<p>Certificate trust stores contain root certificates, each of which is the trust anchor for a PKI. Certificates in trust stores are implicitly trusted by certificate validation software. Vendors' products come pre-populated with many root certificates in their trust stores, including certificates for PKIs that DHS does not want to implicitly trust.</p> <p>DHS Components shall manage the content of installed product's trust stores, including:</p> <ul style="list-style-type: none"> • Leveraging automated management, such as with Microsoft Group Policy Objects (GPOs) • Removing all certificates that have passed their expiration date • Removing all certificates that are no longer trusted • Removing all certificates that are no longer required 	SC-17
5.5.2.v	<p>Commercial products used by DHS and applications developed by DHS that enable the use of PKI shall at a minimum support the following cryptographic algorithms and associated key sizes:</p> <ul style="list-style-type: none"> • SHA 1 • SHA 256 • RSA with 1024 Bit keys • RSA with 2048 bit keys • AES 128 • AES 256 	SC-17

PKI responsibilities are provided in the following table.

Public Key Infrastructure Responsibilities
<p>DHS CISO</p> <p>Provides PKI oversight at the Department level</p> <p>Serves as the DHS PKI Policy Authority</p> <p>Appoints a DHS PKI Operational Authority</p> <p>Creates and maintains a DHS CP that complies with the U.S. Federal CP for the Federal Bridge CA</p> <p>Establishes and maintains the DHS PKI High Assurance Root Certificate Authority (CA)</p> <p>Ensures that all DHS CAs are subordinate to the DHS Root CA</p> <p>Specifies the requirements and process for becoming a subordinate CA</p> <p>Authorizes subordinate CAs</p> <p>Ensures the DHS Root CA cross-certifies with the Federal Bridge CA at the High, Medium, and Basic Assurance levels</p> <p>Ensures that all DHS CAs operate under an approved CPS that complies with the DHS CP</p> <p>Approves Certification Practices Statements for all DHS CAs</p> <p>Ensures that all DHS CAs undergo a compliance audit at least annually, and specifies a DHS PKI Auditor to perform the compliance audits</p> <p>Specifies the DHS PKI Auditor to conduct compliance audits</p> <p>Ensures that appropriate facilities are available for hosting DHS certificate authorities as appropriate for their level of assurance and associated mission. Ensures that appropriate continuity planning is established for all infrastructure that distributes, houses, or stores public keys</p> <p>Ensures that a DHS PKI archive facility is established and maintained to store PKI records</p> <p>Ensures that certificates issued by test, pilot, or other CAs in DHS that are not established as a subordinate CAs to the DHS Root CA shall not be used to protect sensitive DHS operational data, or for authentication on DHS operational systems containing sensitive data</p> <p>DHS Office of Security</p> <p>Ensures that PKI registration activities under its purview are performed in compliance with the applicable CPSs</p> <p>DHS PKI Operational Authority</p> <p>Provides oversight of PKI operations at the Department level</p> <p>Creates and maintains all PKI CPSs pertaining to the DHS PKI</p> <p>Creates and manages DHS PKI Operating Procedures</p> <p>Oversees and reviews management of DHS PKI Operations for each authority certified subordinate to the DHS Root CA</p> <p>Works with DHS and Component physical security entities and/or local registration authorities to oversee the issuance and management of certificates across the DHS enterprise</p>

Public Key Infrastructure Responsibilities
Ensures that all aspects of DHS PKI services, operations and infrastructure related to certificates issued under the DHS CP are in accordance with the requirements, representations, and warranties of the CP
Component CISOs/ISSMs
Ensure that PKI registration activities under their purview are performed in compliance with the applicable CPSs
AOs
Ensure that DHS encryption policy is addressed in the Security Plans for information systems that process sensitive information
ISSOs
Ensure that adequate security measures are in place to protect access to hardware and software
Ensure that new hardware and software has been approved in accordance with the configuration management plan prior to installation
Network/System Administrators
Ensure that DHS cryptographic systems are properly configured and functioning properly

5.5.3 Public Key/Private Key

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

- To encrypt data for that subscriber so that only that subscriber can decrypt it
- To verify that digitally signed data was signed by that subscriber, thereby authenticating the identity of the signing subscriber, and the integrity of the signed data

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

Policy ID	DHS Policy Statements	Relevant Controls
5.5.3.a	DHS FPKI: A single public/private key pair must not be used by a human subscriber for both encryption and digital signature.	SC-12
5.5.3.b	A single public/private key pair must not be used by an NPE for both encryption and digital signature, whenever their separate use is supported by	SC-12

Policy ID	DHS Policy Statements	Relevant Controls
	the protocols native to the NPE.	
5.5.3.c	A authorized human sponsor shall represent each role, group, code-signer, system, application and device subscriber when the subscriber applies for one or more certificates from a DHS CA.	SC-12
5.5.3.d	DHS FPKI: An authorized DHS employee shall sponsor DHS contractors or other affiliates who apply for one or more certificates from a DHS CA.	SC-12
5.5.3.e	A mechanism shall be provided for each DHS CA to enable PKI registrars to determine the eligibility of each proposed human, role, group, code signer, system, application, or device to receive one or more certificates.	SC-12
5.5.3.f	A mechanism shall be provided for each DHS CA to enable PKI registrars to determine and verify the identity of the authorized human sponsor for each DHS contractor, affiliate, role, group, code signer, system, application, or device.	SC-12
5.5.3.g	DHS FPKI: Human subscribers shall not share their private keys and shall be responsible for their security and use. If a human subscriber discloses or shares his or her private key, the subscriber shall be accountable for all transactions signed with the subscriber's private key.	SC-12
5.5.3.h	DHS FPKI: Sponsors for non-human subscribers (systems, application and devices,) shall be responsible for the security of and use of the subscriber's private keys. Every sponsor shall read, understand, and sign a "DHS PKI Device Sponsor Acknowledgement of Responsibilities" as a pre-condition for sponsoring non-human subscribers.	SC-12
5.5.3.i	Subscriber private keys shall not be used by more than one entity, with the following exceptions: <ul style="list-style-type: none"> • Authorized members of a Group Subscriber, may use the Group's private keys. • Multiple systems or devices in a high availability configuration may use a single Key pair providing the Subject Alternative Name (SAN) field within the SSL certificate identifies all of the devices with which the key is to be shared. 	SC-12
5.5.3.j	DHS FPKI: Every human subscriber shall read, understand, and sign a "DHS PKI Human Subscriber Acknowledgement of Responsibilities" as a pre-condition for receiving certificates from a DHS CA. Signed PKI Human Subscriber Agreements shall be maintained by the DHS PKI Registrar.	SC-12

Public key/private key responsibilities are provided in the following table.

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

Public Key/Private Key Responsibilities

Verifies that controls are implemented to hold the sponsor of an organization, application, code signing, or device subscriber responsible for the security of and use of the subscriber's private keys.

Verifies that controls are implemented to maintain individual accountability for each use of a shared organizational or code signing private key.

Ensures that DHS CPSs and Operating Procedures require human subscribers and sponsors to read, understand, and sign DHS PKI Subscriber Agreements as a pre-condition for receiving certificates.

DHS Office of Security

Provides a mechanism, as required by the CPS, to enable PKI registrars to determine the eligibility of each proposed human subscriber to receive one or more certificates from the DHS CA.

Ensures that registrars under their purview require human subscribers and sponsors to read, understand and sign DHS PKI Subscriber Agreements as a pre-condition for receiving certificates.

Component CISOs/ISSMs

Provide a mechanism, as required by the CPS, to enable PKI registrars to determine the eligibility of each proposed human subscriber to receive one or more certificates from the DHS CA.

Provide a mechanism, as required by the CPS, that enables PKI registrars to determine the authorized human sponsor for each organization, application, code signer, or device.

Implement controls to hold human subscribers accountable for the security of their private key and for all transactions signed with their private key.

Implement controls to hold the sponsor of an organization, application, code signing, or device subscriber responsible for the security of and use of the subscriber's private keys.

Implement controls to maintain individual accountability for each use of a shared organizational or code signing private key.

Ensure that registrars under their purview require human subscribers and sponsors to read, understand and sign DHS PKI Subscriber Agreements as a pre-condition for receiving certificates.

ISSOs

Ensure that human subscribers are aware of their responsibilities to protect their private keys.

Ensure that sponsors are aware of their responsibilities to protect the private keys of the subscriber they sponsor.

Maintain auditable records to ensure individual accountability is maintained for each use of an organization or code-signing private key authorized for use by more than one person.

Human Subscribers

Assume responsibility for the security of their private keys.

Abide by their signed DHS PKI Subscriber Agreement for Human Users and review it at least annually.

Sponsors

Public Key/Private Key Responsibilities
Assume responsibility security of the private keys of the subscribers that they sponsor.
Abide by their signed DHS PKI Subscriber Agreement for Sponsors and review it at least annually.

5.6 Malware Protection

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

5.6.1 Types of Malware

Various types of malware are defined in the following table:

<p>Virus – A virus is a self-replicating malicious program segment that attaches itself to legitimate application programs, operating system commands, or other executable system elements and spreads from one system to another. Another definition for virus is: a program or piece of code that is loaded onto a computer without the user’s knowledge and runs against the user’s wishes. As it spreads, it is said to be <i>infecting</i> the system.</p>
--

<p>Worms – Worms are malicious programs that copy themselves from system to system, rather than infiltrating legitimate files. For example, a mass-mailing email worm is a worm that sends copies of itself via email. A network worm makes copies of itself throughout a network or through file shares. Worms often contain Trojan horse or “backdoor” programs.</p>

<p>Logic Bombs – A logic bomb can be defined as dormant code, the activation of which is triggered by a predetermined time or event. For example, a logic bomb might start erasing data files when the system clock reaches a certain date or when an application has been loaded X number of times.</p>

<p>Trojan Horses – A Trojan horse is a computer program that is apparently or actually useful but performs another function covertly. A Trojan horse generally provides remote access to an unauthorized person. A Trojan horse can be used to modify databases, write checks, send email, or destroy files. It could be imbedded by a programmer or downloaded from the Internet.</p>

<p>Web Bugs – A web bug is executable code included in an image (as small as one pixel) that can disrupt the operation of a system or acquire and transmit information from a system without the s knowledge of users who merely visit a malicious or compromised (bugged) web site.</p>

<p>Backdoor – A backdoor is a method of bypassing a system’s security controls. The backdoor may take the form of an installed program or could be a modification to an existing program or hardware device.</p>

5.6.2 How Malware Affects Systems

Malware poses a significant threat to DHS systems therefore, *it is essential that all systems employ preventive measures commensurate with the level of risk identified in the risk analysis.* What makes malware unique is that it can spread from program to program and from system to system *without direct human intervention.*

Systems that can be accessed by DHS-approved browser configurations should be categorized (trusted, untrusted, etc.). Users shall not deploy Web browsers “out of the box,” since the

security policies implemented in such tools tend to reflect vendor interests that do not coincide with DHS interests.

5.6.3 Procedures When Malware Is Detected On a System

If malware is detected, the LAN/system administrator is responsible for taking appropriate actions, including:

- Running disinfectors available with antivirus software
- Scanning backups for malware prior to restoring system applications and data files
- Checking for re-infection from media overlooked during the eradication process
- Using incident reporting procedures described in Section 4.9 to notify the ISSO of the security incident.
- Once the malicious code has been eradicated, the system administrator shall determine the extent of the damage and restore the cleaned programs and files to the disinfected system.

Occurrence of malicious code constitutes a *security incident* that must be reported; reporting procedures are described in Section 4.9, “Security Incidents and Incident Response and Reporting.”

Policy ID	DHS Policy Statements	Relevant Controls
5.6.a	Component CISOs/ISSMs shall establish and enforce Component-level malware protection control policies.	SI-3
5.6.b	Components shall implement a defense-in-depth strategy that: <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 	SI-3
5.6.c	System Owners shall develop and enforce procedures to ensure proper malware scanning of media prior to installation of primary hard drives, software with associated files, and other purchased products.	AC-20, SI-3

Virus protection responsibilities are provided in the following table.

Malware Protection Responsibilities
Component CISOs/ISSMs

Malware Protection Responsibilities

Establish and enforce malware protection control policy

Provide technical expertise and evaluate the effectiveness of malware protection approaches

Security Control Assessors

Ensure that vulnerability to viruses and other malicious code is detailed in the risk analysis section of the Security Authorization Process documentation and that adequate steps to mitigate that risk are taken for each system

System Owners

Assess the impacts associated with system downtime caused by viruses and other malicious code and ensure adequate resources are allocated to address continuity of operations (CO)

System/Network Administrators

Ensure that all DHS systems employ malware protection software

Ensure that malware protection software is installed on every workstation, network, laptop, and mobile computing device

Update malware signature files immediately with each new release

Ensure that malware protection software employs resident scanning

Ensure that malware scanning occurs automatically during boot-up and installation of new software

Ensure that all diskettes are scanned for malware prior to use (including blank disks)

Follow procedures detailed in this manual in the event that malware is detected

ISSOs

Employ malware prevention measures commensurate with the level of risk identified in the risk analysis

Ensure that procedures are implemented to prevent, detect, eradicate, and report computer malware incidents

Ensure that malware incidents are reported in accordance with SOC procedures (see Section 4.9)

Users

Ensure that no files are downloaded or opened from unknown or untrusted sources. All files should be scanned by malware detection software before opening them

Do not open suspicious email

Notify the System / Network Administrator if malware detection software is not installed on the user workstation

Never disable malware detection software functions

Report malware and other malicious code incidents in accordance with procedures described in

Malware Protection Responsibilities
Section 4.9, Security Incidents and Incident Response and Reporting

5.7 Product Assurance

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

The National Information Assurance Partnership (NIAP) is a collaborative effort by NIST and the NSA designed to meet the security testing, evaluation, and assessment needs of both information system producers and consumers. NIAP combines the extensive security experience of both agencies to promote the development of technically sound security requirements for information system products and appropriate metrics for evaluating those products and systems.

The NIAP Common Criteria Evaluation and Validation Scheme for information security (CCEVS) is a partnership between the public and private sectors, to evaluate information system product conformance to international standards. The scheme is designed to help consumers select products that meet their security requirements while helping the manufacturers of those products gain acceptance in the global marketplace.

Compliance with the DHS 4300A Policy Directive, coupled with the requirement that products have been appropriately validated by designated Federal authorities and by CCEVS, will reduce costs and remove the burden of maintaining and providing interoperability between numerous software systems custom written by various contractors.

Policy ID	DHS Policy Statements	Relevant Controls
5.7.a	Information Assurance (IA) shall be considered a requirement for all systems used to input, process, store, display, or transmit sensitive or national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated Commercial off the Shelf (COTS) IA and IA-enabled Information Technology (IT) products. These products shall provide for the availability of systems. The products also shall ensure the integrity and confidentiality of information and the authentication and nonrepudiation of parties in electronic transactions.	---
5.7.b	<p><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:</p> <ul style="list-style-type: none"> - The NIST FIPS validation program - The NSA/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program 	---

Policy ID	DHS Policy Statements	Relevant Controls
	- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement	
5.7.c	The evaluation and validation of COTS IA and IA-enabled products shall be conducted by authorized commercial laboratories or by NIST.	---
5.7.d	Components shall use only cryptographic modules that meet the requirements set forth in Section 5.5, Cryptography.	---
5.7.e	Transaction-based systems (e.g., database management systems and transaction processing systems) shall implement transaction rollback and transaction journaling, or technical equivalents.	CP-10

Product assurance responsibilities are provided in the following table.

Product Assurance Responsibilities
<p>Component CISO/ISSMs Provide guidance in the use of COTS information assurance products</p> <p>Security Control Assessors Validate the proper use of information assurance products</p> <p>System Administrators/ISSOs Ensure selected information assurance products are properly deployed and configured</p> <p>Project Managers Comply with product assurance policy during system development</p>

5.8 Supply Chain

DHS depends on numerous supply chains for the hardware and software needed in order to effectively accomplish its missions. Many of these supply chains are independent of one-another and come with their own set of risks. All programs need to make a risk management decision on how to best manage these risks. It is often no longer enough to perform “due diligence” at the beginning of an acquisition. Effective Supply Chain Risk Management (SCRM) requires the analysis of the Business Impact Assessment (BIA) to determine if the supply chain risks represent unacceptable business impact and what the best cost effective counter-measures are. Because threats to that supply chain are continually evolving, including SCRM into the Continuous Monitoring process will be needed in the near future (e.g., continuous monitoring of integrators or logistics). Some requirements may be included within DHS 4300A and the DHS Information Technology Acquisition Review (ITAR) process, which can respectively serve as

policy and review mechanisms, but incorporation into the greater DHS acquisition process is vital for overall success.

Policy ID	DHS Policy Statements	Relevant Controls
5.8.a	Business Impact Assessments (BIA) shall be used to determine the level of risk introduced to the system by the IT supply chain and whether the IT supply chain threat introduces sufficient risk to require the implementation of countermeasures.	SA-12
5.8.b	To protect against the supply chain threat, Components shall implement appropriate countermeasures, commensurate with the level of risk determined by the BIA.	SA-12

The following table from the NPPD “SCRM Recommendations for 4300A” provides a representative sampling of counter-measures that may be considered:

	Enhancements	SCRM-Unique
Programmatic	<p>Section 3.1.1 – Enhance Information Security Programs with SCRM</p> <ul style="list-style-type: none"> - Include procurement, delivery, storage systems - Enhance risk analysis to include supply chain elements - Enhance access control to include information sharing and integrator/suppliers - Enhance configuration management with identify of SCRM objects - Require technical diversity - Establish integrator/supplier security awareness and training 	<p>Section 3.1.2 – Apply SCRM Countermeasures</p> <ul style="list-style-type: none"> - Require source diversity - Enhanced due diligence for integrator/supplier selection - Enhanced review of integrators/suppliers - Avoid gray market components - Practice anonymous acquisition when acquirer identity is sensitive - All-at-once acquisition of components and spare parts - Limit time between purchase and delivery - Require integrators/suppliers test components - Require flaw detection and remediation - Require an independent witness for some testing - Require integrators/suppliers document testing - Recursive requirements for integrators/suppliers
Technical	<p>Section 3.1.3 – Enhance Technical and Operational Countermeasures with SCRM</p> <ul style="list-style-type: none"> - Enhanced access control for integrators/suppliers - Enhanced intrusion detection and response - Enhanced acceptance testing - Enhanced disposal requirements - Enhanced continuous monitoring - Enhanced ISCM to integrate data collection - Enhanced review of integrator/supplier procedures 	<p>Section 3.1.4 – Apply SCRM Countermeasures</p> <ul style="list-style-type: none"> - Employ formal and accountable transit, storage, and delivery procedures - Limit transit and storage of critical components to trusted channels/services - Specify use of a code analyzer prior to compilation - Use code signatures - Use/specify tamper-proof or tamper-evident packaging - Enable forensic analysis in system/component design

6.0 DOCUMENT CHANGE REQUESTS

Changes to "DHS Sensitive Systems Policy Directive 4300A" and to the *DHS 4300A Sensitive Systems Handbook* may be requested in accordance with Section 1.7, "Changes to Policy."

7.0 QUESTIONS AND COMMENTS

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

APPENDIX A ACRONYMS AND ABBREVIATIONS

Acronym	Meaning
3-DES	Triple Data Encryption Standard
ACD	Automatic Call Distribution
AES	Advanced Encryption Standards
AIS	Automated Information System
A-Number	Alien Registration Number
AO	Authorizing Official
APO	Army Post Office
ARB	Acquisition Review Board
ATO	Authority to Operate
BI	Background Investigation
BIA	Business Impact Assessment
BLSR	Baseline Security Requirements
CA	Certification Authority
CBP	Customs and Border Protection
CCB	Change Control Board
CCE	Common Configuration Enumeration
CD	Compact Disk
CFO	Chief Financial Officer
CI	Counter-Intelligence
CIFS	Common Internet File Service
CIO	Chief Information Officer
CISID	Chief, Internal Security and Investigations Division
CISID-OIS	Chief, Internal Security and Investigations Division, Office of Security
CISO	Chief Information Security Officer
CM	Configuration Management
CMG	Core Management Group
CMP	Configuration Management Plan
CO	Continuity of Operations

Acronym	Meaning
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan Continuity of Operations Planning
COTS	Commercial off the Shelf
CP	Contingency Plan Contingency Planning Certificate Policy
CPE	Common Platform Enumeration
CPIC	Capital Planning and Investment Control
CPS	Certificate Practices Statement
CRC	Cyclical Redundancy Check
CRE	Computer-Readable Extract
CRL	Certificate Revocation List
CSID-OIS	Chief, Internal Security and Investigations Division, Office of Security
CSO	Chief Security Officer
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
DES	Digital Encryption Standards
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DNSSEC	Domain Name System Security Extensions
DOD	Department of Defense
DoS	Denial of Service
DoT	Department of Treasury
DR	Disaster Recovery
DT&E	Development Test and Evaluation
DVD	Digital Video Disk
EA	Enterprise Architecture
EAB	Enterprise Architecture Board
EO	Executive Order

Acronym	Meaning
FAM	Foreign Affairs Manual
FBCA	Federal Bridge Certification Authority
FDCC	Federal Desktop Core Configuration (term now obsolete, replaced by U.S. Government Configuration Baseline (USGCB))
FEMA	Federal Emergency Management Agency
FICAM	Federal Identity, Credentialing, and Access Management
FIPS	Federal Information Processing Standard
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
FOIA	Freedom of Information Act
FPGA	Field Programmable Gate Array
FPKI PA	Federal PKI Policy Authority
FTP	File Transfer Protocol
FYHSP	Future Years Homeland Security Program
GSA	General Services Administration
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
HSAR	Homeland Security Acquisition Regulations
HSDN	Homeland Secure Data Network
HSPD	Homeland Security Presidential Directive
HVAC	Heating, Ventilation and Air Conditioning
I&A	Intelligence and Analysis
IA	Identification and Authentication Information Assurance
IATO	Interim Authority to Operate
IAVA	Information Assurance Vulnerability Assessment
ICAM	Identity, Credentialing, and Access Management
ICAT	Internet Categorization of Attacks Toolkit

Acronym	Meaning
ICE	Immigration and Customs Enforcement
IDF	Intermediate Distribution Frame
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IOC	Initial Operating Capability
IPT	Integrated Product Team
IR	Incident Response Infrared
IRB	Investment Review Board
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISA	Interconnection Security Agreement
ISP	Internet Service Provider
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISVA	Information Security Vulnerability Alert
ISVB	Information Security Vulnerability Bulletin
ISVM	Information System Vulnerability Management
IT	Information Technology
ITAR	Information Technology Acquisition Review
ITGC	Information Technology General Controls
IXC	Inter-exchange Carrier
JWICS	Joint Worldwide Intelligence Communications System
KDP	Key Decision Point
LAN	Local Area Network
LBI	Limited Background Investigation
LE	Law Enforcement
LEC	Local Exchange Carrier
LMR	Land Mobile Radio
MA	Major Application

Acronym	Meaning
MBI	Minimum Background Investigation
MD	Management Directive
MDF	Main Distribution Frame
MMS	Multimedia Messaging Service
MO	Magneto Optical
NAC	National Agency Check
NACIC	National Agency Check and Inquiries and Credit
NACLC	NAC with Law and Credit
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
NLT	No Later Than
NOC	Network Operations Center
NPPD	National Protection and Programs Directorate
NSA	National Security Agency
NSF	Nonstandard Facilities
OCIO	Office of the Chief Information Officer
OID	Object identifier
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPA	Office of Public Affairs
OPM	Office of Personnel Management
OT&E	Operational Test and Evaluation
OTAR	Over-The-Air-Rekeying
PBX	Private Branch Exchange
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications Services
PDA	Personal Digital Assistant

Acronym	Meaning
PED	Portable Electronic Device
PEP	Policy Enforcement Point
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identity Number
PIRT	Privacy Incident Response Team
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PKI PA	PKI Policy Authority
PKI MA	PKI Management Authority
PM	Program Manager
PNS	Protected Network Services
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPOC	Privacy Point of Contact
PSTN	Public Switched Telephone Network
PTA	Privacy Threshold Analysis
RA	Risk Assessment Registration Authority
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFID	Radio Frequency Identification
RMS	Risk Management System
ROB	Rules of Behavior
ROM	Read Only Memory
RTM	Requirements Traceability Matrix
SA	Security Architecture

Acronym	Meaning
SAISO	Senior Agency Information Security Officer
SAN	Subject Alternative Name
SAOP	Senior Agency Official for Privacy
SAR	Security Assessment Report
SCAP	Security Content Automation Protocol
SCI	Sensitive Compartmented Information
SCRM	Supply Chain Risk Management
SELC	Systems Engineering Life Cycle
SFTP	Secure File Transfer Protocol
SIM	Security Incident Management
SLA	Service Level Agreement
SMS	Short Message Service
SOC	Security Operations Center
SOC CONOPS	Security Operations Center Concept of Operations
SORN	System of Records Notice
SOW	Statement of Work
SP	Special Publication (only in titles of NIST publications, e.g. SP 800-37) Security Plan
SSBI	Single Scope Background Investigation
SSH	Secure Shell
SSL	Secure Socket Layer
SSP	Shared Service Provider
Stat.	Statute (refers to a law found in <i>U.S. Statutes at Large</i>)
TA	Technical Advisory
TAF	Trusted Agent FISMA
TCP	Transport Control Protocol
TCP/IP	Transport Control Protocol/Internet Protocol
TFPAP	Trust Framework Provider Adoption Process
TIA/EIA	Telecommunications Industry Association/Electronic Industries Alliance

Acronym	Meaning
TIC	Trusted Internet Connections
TOS	Terms of Service
TRM	Technical Reference Model
TS	Top Secret
TS/SCI	Top Secret, Sensitive Compartmented Information
TSA	Transportation Security Administration
UCMJ	Uniform Code of Military Justice
UDP	User Datagram Protocola
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
USC	United States Code (in citations of codified U.S. law)
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Service
USGCB	U.S. Government Configuration Baseline
USSS	United States Secret Service
VA	Vulnerability Assessment
VAT	Vulnerability Assessment Team
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WORM	Write Once Read Many
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network

APPENDIX B GLOSSARY

The following definitions apply to the policies and procedures outlined in this document. Other definitions may be found in National Institute of Standards and Technology (NIST) IR 7298, “Glossary of Key Information Security Terms” and in the “National Information Assurance (IA) Glossary.”

Acceptable Risk	Mission, organizational, or program-level risk deemed tolerable by the Risk Executive after adequate security has been provided.
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. [OMB Circular A-130, Appendix III]
Annual Assessment	Department of Homeland Security (DHS) activity for meeting the annual Federal Information Security Management Act (FISMA) self-assessment requirement.
Authorization Package	<p>The documents submitted to the AO for the Authorization Decision. An Authorization Package consists of:</p> <ul style="list-style-type: none"> Authorization Decision Letter Security Plan - criteria provided on when the plan should be updated Security Assessment Report - updated on an ongoing basis whenever changes are made to either the security controls in the information system or the common controls inherited by those systems Plan of Action and Milestones (POA&M)
Authorizing Official (AO)	An official within a Federal Government agency empowered to grant approval for a system to operate.
Certification/ Certifying Agent	A contractor that performs certification tasks as designated by the CO.
Certificate (or Certifying) Authority (CA)	A trusted third party that issues certificates and verifies the identity of the holder of the digital certificate.
Chief Information Officer (CIO)	The executive within a Federal Government agency responsible for its information systems.
Compensating Control	An internal control intended to reduce the risk of an existing or potential control weakness.

Component	A DHS Component is any of the entities within DHS, including every DHS office and independent agencies.
Computer Security Incident Response Center	DHS organization that responds to computer security incidents.
Designated Approval Authority (DAA)	Obsolete term; see Authorizing Official (AO).
Enterprise Operations Center (SOC)	The DHS organization that coordinates security operations for the DHS Enterprise.
Exception	Acceptance to permanently operate a system that does not comply with policy.
For Official Use Only (FOUO)	The marking instruction or caveat “For Official Use Only” will be used within the DHS community to identify sensitive but unclassified information that is not otherwise specifically described and governed by statute or regulation.
General Support System (GSS)	An interconnected set of information resources under the same direct management control and sharing common functionality. A GSS normally includes hardware, software, information, applications, communications, data, and users.
Information Security Vulnerability Management (ISVM)	A DHS system that provides notification of newly discovered vulnerabilities, and tracks the status of vulnerability resolution.
Information System	Any information technology that is (1) owned, leased, or operated by any DHS Component, (2) operated by a contractor on behalf of DHS, or (3) operated by another Federal, state, or local Government agency on behalf of DHS. Information systems include general support systems and major applications (MA).
Information System Security Officer (ISSO)	A Government employee or contractor who implements and/or monitors security for a particular system.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Major Application (MA)	<p>An automated information system (AIS) that “requires special attention to security due to the risk and magnitude of harm that can result from the loss, misuse, or unauthorized access to or modification of the information in the application” in accordance with OMB Circular A-130.</p> <p>An MA is a discrete application, whereas a GSS may support multiple applications.</p>
Management Controls	The security controls for an information system that focus on the management of risk and the management of information system security.
Operational Controls	The security controls for an information system that are primarily implemented and executed by people (as opposed to being executed by systems).
Operational Risk	The risk contained in a system under operational status. It is the risk that an AO accepts when granting an ATO.
Personally Identifiable Information (PII)	Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to an individual regardless of whether the individual is a U.S. Citizen, legal permanent resident, or a visitor to the U.S.
Pilot	A test system in the production environment that may contain operational data and may be used to support DHS operations, typically in a limited way.
Policy Enforcement Point (PEP)	A firewall or similar device that can be used to restrict information flow.
Policy Statement	A high-level rule for guiding actions intended to achieve security objectives.
Portable Electronic Device (PED)	A device that has a battery and is meant to process information without being plugged into an electric socket; it is often handheld but can be a laptop computer.
Privacy Sensitive System	Any system that collects, uses, disseminates, or maintains PII or sensitive PII.
Production	The applications and systems that DHS end users access and use operationally to execute business transactions.
Prototype	A test system in a test environment that must not contain operational data and must not be used to support DHS operations.
Remote Access	Access to a DHS information system by a user (or an information system) communicating through an external, non-DHS-controlled network (e.g., the Internet).

Residual Risk	The risk remaining after security controls have been applied.
Risk Executive (RE)	An individual who ensures that risks are managed consistently across the organization. An RE can be at the Departmental or Component level.
Security Control	A particular safeguard or countermeasure to protect the confidentiality, integrity, and availability of a system and its information.
Security Control Assessor	A senior management official who certifies the results of the security control assessment. He or she must be a Federal Government employee.
Security Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Security Operations Center (SOC)	The organization in each DHS Component that coordinates the Component's security operations.
Security Requirement	A formal statement of action or process applied to an information system and its environment in order to provide protection and attain security objectives. Security requirements for any given system are contained in its Security Plan.
8.0 Senior Agency Information Security Official (SAISO)	The point of contact within a Federal Government agency responsible for its information system security.
Sensitive But Unclassified	Obsolete designation; see Sensitive Information.
Sensitive Information	Information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal Government programs or other programs or operations essential to the national interest.
Sensitive Personally Identifiable Information (Sensitive PII)	PII that requires stricter handling guidelines because of the nature of the data and the increased risk to an individual if compromised, and if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of sensitive PII include Social Security numbers and Alien Registration Numbers (A-number).
Significant Incident	A computer security-related incident that represents a meaningful threat to the DHS mission and requires immediate leadership notification.

Spam	Emails containing unwanted commercial solicitation, fraudulent schemes, and possibly malicious logic.
Strong Authentication	Layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information.
System	A discrete set of information system assets contained within the authorization boundary.
System Owner	The agency official responsible for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.
Technical Controls	The security controls for an information system that are primarily implemented and executed by the information system through mechanisms contained in system hardware, software, or firmware.
Two-Factor Authentication	Authentication can involve something the user knows (e.g., a password), something the user has (e.g., a smart card), or something the user “is” (e.g., a fingerprint or voice pattern). Single-factor authentication uses only one of the three forms of authentication, while two-factor authentication uses any two of the three forms. Three-factor authentication uses all three forms.
Unclassified Information	Information that has not been determined to be classified pursuant to Executive Order 13526, as amended.
USB Device	A device that can be connected to a computer via a USB port.
USB Drive	A memory device small enough to fit into a pocket that connects to a computer via a USB port.
Vulnerability Scanning	An automated scan for potential security vulnerabilities.
Waiver	Temporary dispensation of a policy requirement, granted to a Component to operate a system while working toward compliance.

APPENDIX C REFERENCES

The DHS information security program and organization are based upon public laws, executive orders, national policy, external guidance, and internal DHS guidance.

Public Laws and U.S. Code

- Privacy Act of 1974, as amended, Public Law 93-579, codified at 5 USC 552a
- E-Government Act of 2002, including Title III, Federal Information Security Management Act (FISMA), Public Law 107-347, codified at 44 USC. §§ 3541-3549
- Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], Public Law 104-106, codified at 5 CFR *CFR* § 2635, Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch
- Computer Security Act of 1987 as amended, Public Law 100-235, codified at 40 USC 759.
- Freedom of Information Act of 2002, as amended, Public Law 89-554, 80 Stat 383, amended 1996, 2002, 2007

Executive Orders

- Executive Order 12958, “Classified National Security Information,” March 25, 2003
- Homeland Security Presidential Directive 12, “Policy for a Common Identification Standard for Federal Employees and Contractors,” August 27, 2004

Office of Management and Budget Directives

- Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” revised, November 30, 2000
- OMB Bulletin 06-03, “Audit Requirements for Federal Financial Statements,” August 23, 2006
- OMB Memorandum M-04-04, “E-Authentication Guidance for Federal Agencies,” December 16, 2003
- OMB Memorandum M-06-15, “Safeguarding Personally Identifiable Information,” May 22, 2006
- OMB Memorandum M-06-16, “Protection of Sensitive Agency Information,” June 23, 2006
- OMB Memorandum M-07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” May 22, 2007
- OMB Memorandum M-09-02, “Information Technology Management Structure and Governance Framework,” October 21, 2008
- OMB Memorandum 10-15, “FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, April 21, 2010

- OMB Memorandum 10-28, “Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS),” July 6, 2010
- OMB Memorandum 11-06, “WikiLeaks - Mishandling of Classified Information,” November 28, 2010

Other External Guidance

- Intelligence Community Directive Number 508, “Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation,” September 15, 2008
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS), including:
 - NIST FIPS 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006”
 - NIST FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems,” February 2004
- NIST Information Technology Security Special Publications (SP) 800 series, including:
 - NIST SP 800-16, Rev 1, “Information Technology Security Training Requirements: A Role- and Performance-Based Model (Draft),” April 1998
 - NIST SP 800-34, Rev 1, “Contingency Planning Guide for Information Technology Systems,” May, 1010
 - NIST SP 800-37, Rev 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,” February 2010
 - NIST SP 800-39, “Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View,” March 2011
 - NIST SP 800-50, “Building an Information Technology Security Awareness and Training Program,” October 2003
 - NIST SP 800-52, “Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations,” June 2005
 - NIST SP 800-53, Rev 3, “Recommended Security Controls for Federal Information Systems and Organizations,” August 2009, with updated errata May 01, 2010”
 - NIST SP 800-53A, Rev 1, Guide for Assessing the Security Controls in Federal Information Systems,” June 2010
 - NIST SP 800-60, Rev 1, “Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices,” August 2008
 - NIST SP 800-63, Rev 1, Draft 3“Electronic Authentication Guideline, June 2011

- NIST SP 800- 65, Rev 1, Draft, “Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process (CPIC),” July 14, 2009
- NIST SP 800-88, “Guidelines for Media Sanitization,” Sept 2006
- NIST SP 800-92, “Guide to Computer Security Log Management,” September 2006
- NIST SP 800-94, “Guide to Intrusion Detection and Prevention Systems (IDPS),” February 2007
- NIST SP 800-95, “Guide to Secure Web Services,” August 2007
- NIST SP 800-100, “Information Security Handbook: A Guide for Manager,” October 2006
- NIST SP 800-115, “Technical Guide to Information Security Testing and Assessment,” November 2008
- NIST SP 800-118, Draft, “Guide to Enterprise Password Management (Draft),” April 21, 2009
- NIST SP 800-122, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),” April 2010
- NIST SP 800-123, “Guide to General Server Security,” July 2008
- NIST SP 800-124, “Guidelines on Cell Phone and PDA Security,” October 2008
- NIST SP 800-128, “Guide for Security Configuration Management of Information Systems (Draft),” August 2011
- NIST SP 800-137, “Information Security Continuous Monitoring for Federal Information Systems and Organizations,” September 2011
- NIST Interagency or Internal Reports (NISTIR)
 - NIST IR 7298 Rev 1, “Glossary of Key Information Security Terms,” February 2011
- Committee on National Security Systems (CNSS) Instructions
- CNSS Instruction No. 4009 (Revised), “National Information Assurance Glossary,” April 2010
- CNSS Instruction No. 1001, “National Instruction on Classified Information Spillage,” February 2008

Internal Guidance

- “Department of Homeland Security Acquisition Regulation (HSAR),” 48 CFR Chapter 30, June 2006
- **DHS Management Directives (MD), especially:**

- MD 140-01, "[Information Technology Systems Security](#)," July 31, 2007
- MD 11042.1, "[Safeguarding Sensitive but Unclassified \(For Official Use Only\) Information](#)," January 6, 2005
- MD 1030, "[Corrective Action Plans](#)," May 15, 2006
- MD 4400.1, **DHS Web** (Internet, Intranet, and Extranet Information) and Information Systems," March 1, 2003
- MD 4500.1, "[DHS Email Usage](#)," March 1, 2003
- MD 4600.1, "[Personal Use of Government Office Equipment](#)," April 14, 2003
- MD 4900, "[Individual Use and Operation of DHS Information Systems/Computers](#)," document undated
- DHS Instruction 121-01-007, "[Personnel Suitability and Security Program](#)," June 2009
- DHS Directive 102-01, "Acquisition Management," January 20, 2010

APPENDIX D DOCUMENT CHANGE HISTORY

Version	Date	Description
0.1	December 13, 2002	Draft Baseline Release
0.2	December 30, 2002	Revised Draft
0.5	January 27, 2003	Day One Interim Policy
1.0	June 1, 2003	Department Policy
1.1	December 3, 2003	Updated Department Policy
2.0	March 31, 2004	Content Update
2.1	July 26, 2004	Content Update
2.2	February 28, 2005	Content Update
2.3	March 7, 2005	Content Update
3.0	March 31, 2005	Includes updates to PKI, Wireless Communications, and Media Sanitization (now Media Reuse and Disposition) sections
3.1	July 29, 2005	New policies: 3.1b,e,f, 3.1g, 4.1.5b, 4.8.4a. Modified policies: 3.7b, c, 3.9b,g, 3.10a, 4.3.1b, 4.8.2a, 4.8.5e, 5.1.1b, 5.2.2a, 5.3a, c, 5.4.1a, 5.4.5d, 5.4.8c, 5.5.1a, 5.7d. Policies relating to media disposal incorporated into policies within Media Reuse and Disposition section. Deleted policy regarding use of automated DHS tool for conducting vulnerability assessments.
3.2	October 1, 2005	Modified policies 3.8b, 4.8.1a, 5.2.1a&b, 5.2.2a, and 5.4.3c; combined (with modifications) policies 4.1e and 4.1f; modified Section 1.5
3.3	December 30, 2005	New policies: policies 3.9a–d; 3.11.1b; 4.3.1a; 4.6c; 5.4.3d&e. Modified policies: policies 3.9i&j; 4.3.2a; 4.6a, b; 4.6.1e; 4.6.2j; 4.6.2.1a; 4.6.3e; 5.4.3c; 5.5.2k. Modified sections: 2.5, 2.7, 2.9, 2.11, 3.9, 5.5.2.
4.0	June 1, 2006	New policies: 3.5.3.c&g, 4.6.2.3.c, 5.1.c, 5.2.c, 5.4.1.a. Modified policies: 3.5.1.c, 3.5.3.d–f, 3.7.a&b, 3.9.a&b, d, 4.1.4.b&c, 4.2.1.a, 4.3.1.a, 4.6.c, 4.6.1.a, 4.6.2.f, 4.10.3.a, 5.2.1.b, 5.3.a&b, 5.4.1.b, 5.4.3.c, 5.4.5.d. Modified section: Section 2.9.
4.1	September 8, 2006	New policies: 3.14.1.a–c; 3.14.3.a–c; 4.10.1.c; 5.3.d&e; 5.4.1.c–e. Modified policies: 3.9.b; 4.6.2.d; 4.8.2.a–c; 4.10.1.b; 5.1.c; 5.3.c; 5.4.1.b. New sections: 3.14, 3.14.1, 3.14.3. Modified sections: 2.9, 4.8.2.
4.2	September 29, 2006	New policies: 4.6.4.a–f. Modified policies: 4.3.3.a–c. New section: 4.6.4.
5.0	March 1, 2007	New policies: 4.1.5.h. Modified policies: 3.10.c, 4.1.1.d, 4.1.5.a,b,f, &g,

Version	Date	Description
		4.6.2.d, 4.6.3.f, 5.2.c, 5.4.8.a, 5.6.b. New sections: 4.1.1. Modified sections: 1.2, 1.4.2, 1.4.3, 2.9, 3.12, 4.1 and subsections, 4.6.1–4.6.4, 4.9, 5.2.1. Renumbered sections: 4.1.2–4.1.6, 4.9, 4.10, 4.11, 4.12.
5.1	April 18, 2007	Update based on SOC CONOPS, Final Version 1.4.1, April 6, 2007; Adds DHS Chief Financial Officer – Designated Financial Systems; Updates the term, <i>Sensitive But Unclassified</i> to <i>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> <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>
6.0	May 17, 2008	<p>Global change</p> <p>"Shoulds" changed to "shalls" throughout the document. Replaced certain instances of "will" with "shall" throughout document to indicate compliance is required.</p> <p>Various changes were made throughout the document to ensure that the</p>

Version	Date	Description
		<p>4300A Policy and Handbook align with the 4300B Policy and Handbook.</p> <p>“ISSM” changed to “CISO/ISSM” throughout the document.</p> <p>"CPO" changed to "Chief Privacy Officer" throughout the document.</p> <p>“IT Security Program” changed to “Information Security Program” throughout the document.”</p> <p>“System Development Life Cycle” changed to “System Life Cycle” and “SDLC” changed to “SLC” throughout the document.</p> <p>Title Page</p> <p>Title page of 4300A Policy - Language on the Title Page was reworded.</p> <p>“This is the implementation of DHS Management Directive 4300.1.”</p> <p>Section 1.0</p> <p>1.1 – Updated to clarify 90 day period in which to implement new policy elements.</p> <p>1.2 – Added OMB, NIST, and CNSS references.</p> <p>1.4 – Added reference and link to Privacy Incident Handling Guidance and the Privacy Compliance documentation.</p> <p>1.4.2 – Added definition of National Intelligence Information.</p> <p>1.4.3 – Inserted definition of National Security Information to align with 4300B Policy.</p> <p>1.4.8.1 – Definition of General Support System was updated.</p> <p>1.4.8.2 – Definition of Major Application was updated.</p> <p>1.4.10 – Section was renamed “Trust Zone.”</p> <p>1.4.16 – Inserted new definition for FISMA.</p> <p>1.5 – Language was updated to increase clarity for financial system owners for waivers and exceptions.</p> <p>Section 2.0</p> <p>2.3 – Added a new responsibility for DHS CIO.</p> <p>2.4 – Added a new responsibility for Component CIOs.</p> <p>2.5 - Chief Information Security Officer (CISO) renamed DHS Chief Information Security Officer (CISO). Updated to include privacy-related</p>

Version	Date	Description
		<p>responsibilities.</p> <p>2.6 – Added a new section in Roles and Responsibilities called “Component CISO.”</p> <p>2.7 – Updated Component ISSM Role and Responsibilities.</p> <p>2.8 – Changed name of the section from "Office of the Chief Privacy Officer (CPO)" to "The Chief Privacy Officer". Updated to include privacy-related responsibilities.</p> <p>2.9 – Added a new role for DHS CSO.</p> <p>2.10 – Updated to include privacy-related responsibilities.</p> <p>2.11 - Added privacy-related responsibilities.</p> <p>2.12 – Added a new section, “OneNet Steward.”</p> <p>2.13 – Added a new section, “DHS Security Operations Center (DHS SOC) and Computer Security Incident Response Center (CSIRC).”</p> <p>2.14 – Added a new section, “Homeland Secure Data Network (HSDN) Security Operations Center (SOC).”</p> <p>2.16 – Added a new section, “Component-level SOC.”</p> <p>2.18 – Updated to include privacy-related responsibilities.</p> <p>2.19 – Last sentence of first paragraph has been updated to say: “ISSO Duties shall not be assigned as a collateral duty. Any collateral duties shall not interfere with their ISSO duties.”</p> <p>2.20 – Updated to include privacy-related responsibilities.</p> <p>Section 3.0</p> <p>3.9 – Added C&A information for unclassified, collateral classified and SCI systems. Also, prior to DHS Policy table, included sentence regarding C&A.</p> <p>3.9.b – Language updated to clarify that a minimum impact level of moderate is required for confidentiality for CFO designated financial systems.</p> <p>3.9.h – New guidance is provided to clarify short term ATO authority.</p> <p>3.11.1 – Added new section discussing the CISO Board.</p> <p>3.11.3 – Removed DHS Wireless Security Working Group.</p> <p>3.14.1 – Added new text defining PII and sensitive PII. At the end of bullet #4, added definition of computer-readable data extracts. Updated 3.14.1.a</p>

Version	Date	Description
		<p>and 3.14.1.b based on input from the Privacy Office. Added sentence “DHS has an immediate goal that remote access should only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.</p> <p>3.14.2 - Added new section called "Privacy Threshold Analyses."</p> <p>3.14.3 - Updated Privacy Impact Assessment Responsibilities table.</p> <p>3.14.4 - Added new section called "System of Record Notices."</p> <p>Section 4.0</p> <p>4.1.5.c – Updated to address training requirements.</p> <p>4.1.5.g – Deleted “Training plans shall include awareness of internal threats and basic IT security practices.”</p> <p>4.1.5.h (now 4.1.5.g) – Updated to include the following sentence: “Components shall account for Contingency Plan Training, and Incident Response Training conducted for Moderate and High IT Systems.”</p> <p>4.3.1.d – FIPS 140-2 compliance language was updated.</p> <p>4.8.1.a and 4.8.1.c – Language has been updated to provide clarification of timeout values.</p> <p>4.8.2.a – FIPS 140-2 compliance language was updated.</p> <p>4.8.2.b – Added a new policy element regarding powering down laptops when not in use.</p> <p>4.9 – Section was renamed “Department Information Security Operations.”</p> <p>4.9, 4.9.1, 4.9.2 – Updated policy elements to support Department security operations capabilities, based on the SOC CONOPS.</p> <p>4.9.2.b – Updated to say “Components shall obtain guidance from the DHS SOC before contacting local law enforcement except where there is risk to life, limb, or destruction of property.”</p> <p>4.12.a – Added policy element to align with Handbook.</p> <p>Section 5.0</p> <p>5.2.1.a, 5.2.1.b, and 5.2.1.c – Language has been updated to provide clarification of timeout values.</p> <p>5.2.2 Introductory language, 5.2.2.a, 5.2.2.b, and 5.2.2.c – Language and policy updated to clarify the meaning of a session termination.</p> <p>5.3.f - Updated to clarify responsibilities of the System Owner regarding</p>

Version	Date	Description
		<p>computer-readable data extracts.</p> <p>5.4.1.d – Added sentence “DHS has an immediate goal that remote access should only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.”</p> <p>5.4.3.a through i – New guidance is provided regarding the preparation of ISAs for interconnections to the DHS OneNetwork.</p> <p>5.4.3.g – Replaced “interconnect service agreements” with “interconnection security agreements.”</p> <p>5.4.4.f - New guidance is provided regarding internal firewalls.</p> <p>5.4.5.f – New guidance is provided regarding the use of the RDP protocol.</p> <p>5.4.6 – Added text “NOTE: Due to many attacks that are HTML-based, please note that DHS will be following the lead of the DoD and moving to text based email.”</p> <p>5.4.8.a – Language updated to reflect that annual vulnerability assessments should be conducted.</p> <p>5.4.8.f – Policy updated to clarify automated system scanning.</p> <p>5.5.1.c – Updated element to specify usage of cryptographic modules that “are FIPS 197 compliant and have received FIPS 140-2 validation.”</p> <p>5.5.2.f – Policy updated to clarify hosting of DHS Root CA.</p>
6.1	September 23, 2008	<p>Global Changes</p> <p>Replaced all instances of “CISO/ISSM” with “Component CISO/ISSM.”</p> <p>Replaced all DHS-related instances of “agency/agency-wide” with “Department/Department-wide.”</p> <p>Replaced all instances of “24x7” with “continuous” or “continuously,” as appropriate.</p> <p>Replaced all instances of “IT security” with “information security.”</p> <p>Various minor editorial and grammatical changes were made throughout the document.</p> <p>Section 1.0</p> <p>1.2 – Added reference to E-Government Act of 2002, January 7, 2003.</p> <p>1.4 – Replaced “National InfoSec Glossary” with “National Information Assurance (IA) Glossary.”</p>

Version	Date	Description
		<p>1.4.5 – Replaced third sentence with “System vulnerability information about a financial system shall be considered Sensitive Financial Information.”</p> <p>1.5.2 – Added text regarding acceptance of resulting risk by the Component CFO for financial systems.</p> <p>1.5.3 – Corrected the title and location of Attachment B. Added text regarding PTA requirements.</p> <p>Section 2.0</p> <p>2.1 – Updated to clarify Secretary of Homeland Security responsibilities.</p> <p>2.2 – Updated to clarify Undersecretaries and Heads of DHS Components responsibilities.</p> <p>2.3 – Updated to clarify DHS CIO responsibilities.</p> <p>2.4 – Updated to clarify Component CIO responsibilities.</p> <p>2.5 – Updated to clarify DHS CISO responsibilities.</p> <p>2.6 – Updated to clarify Component CISO responsibilities.</p> <p>2.8 – Moved “The Chief Privacy Officer” section to 2.9.</p> <p>2.11 – Updated to clarify Program Managers’ responsibilities.</p> <p>2.14 – Updated to clarify HSDN SOC responsibilities. Updated HSDN SOC unclassified email address.</p> <p>2.19 – Updated to clarify ISSO responsibilities and the assignment of ISSO duties as a collateral duty.</p> <p>2.20 – Updated to clarify System Owners’ responsibilities.</p> <p>2.23.2 – Updated to clarify DHS CIO responsibilities for financial systems.</p> <p>Section 3.0</p> <p>3.1.e – Replaced “FISMA and OMB requirements” with “FISMA, OMB, and other Federal requirements.”</p> <p>3.1.h – Replaced “maintain a waiver” with “maintain a waiver or exception.”</p> <p>3.14.1 – Included text regarding the type of encryption needed for laptops.</p> <p>3.14.3 – Included text stating that the PTA determines whether a PIA is conducted.</p> <p>3.14.4 – Moved first sentence of second paragraph to be the first sentence of</p>

Version	Date	Description
		<p>the first paragraph. Included “that are a system of record” after “IT Systems” in the second sentence of the first paragraph.</p> <p>Section 4.0</p> <p>4.3.1.a – Included “locked tape device” in media protection.</p> <p>4.3.1.d – Updated to clarify that AES 256-bit encryption is mandatory.</p> <p>4.8.2.a – Updated to clarify that AES 256-bit encryption is mandatory.</p> <p>4.8.3.c – Included new policy element regarding use of seized IT equipment.</p> <p>4.8.4.f – Included new policy element regarding management and maintenance of system libraries.</p> <p>4.8.5.b – Policy updated to clarify limited personal use of DHS email and Internet resources.</p> <p>4.9 – First paragraph updated to clarify DHS SOC and HSDN SOC responsibilities.</p> <p>4.9.b – Updated to specify that the HSDN SOC is subordinate to the DHS SOC.</p> <p>4.9.1 – First two paragraphs updated to clarify relationship between the DHS SOC and the HSDN SOC.</p> <p>4.9.1.a – Removed the words “Component SOC.”</p> <p>4.9.1.b – Updated to clarify means of communication for reporting significant incidents.</p> <p>4.9.1.c – Updated to clarify the length of time by which significant HSDN incidents must be reported.</p> <p>4.9.1.d. – Updated to clarify reporting for HSDN incidents.</p> <p>Section 5.0</p> <p>5.2.d – Replaced “Component CISO/ISSM” with “Component CISO/ISSM or his/her designee.”</p> <p>5.2.1 – Changed “48 hour time period” to “24 hour time period.”</p> <p>5.4.5.g – Included new policy element regarding blocking of specific Internet websites or categories.</p> <p>5.4.7 – Updated the policy element to prohibit use of webmail and other personal email accounts.</p> <p>5.5.1.c – Updated to clarify that AES 256-bit encryption is mandatory.</p>

Version	Date	Description
		<p>5.7.d – Included new policy element regarding use of cryptographic modules in order to align with 4300A Handbook.</p> <p>5.7.e – Included new policy element regarding rollback and journaling for transaction-based systems.</p>
6.1.1	October 31, 2008	5.2.3 – Included new language and a link to the DHS computer login warning banner text on DHS Online.
7.0		<p>General Updates</p> <p>Added section and reference numbers to policy elements</p> <p>Added NIST 800-53 reference controls to policy elements</p> <p>Added hyperlinks to most DHS references</p> <p>Introduced new terminology Senior Agency Information Security Officer, Risk Executive, and Authorizing Official (AO) – replaces DAA, as per NIST 800-37 and 800-53</p> <p>Added Appendix A – Acronyms</p> <p>Added Appendix B – Glossary</p> <p>Added Appendix C – References list has been updated and moved to Appendix C. (these are detailed references, an abbreviated list is still found at the beginning of the document)</p> <p>Added Appendix D – Change History (This was moved from the front of the document)</p> <p>Specific Updates</p> <p>Section 1.1 – Information Security Program Policy – Added the statement, “Policy elements are designed to be broad in scope. Specific implementation information can often be found in specific National Institute for Standards and Technology (NIST) publications, such as NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Systems.”</p> <p>Section 1.4.17-19 – Privacy – Added definitions for PII, SPII, and Privacy Sensitive Systems</p> <p>Section 1.5 – Exceptions and Waivers – Updated this section, clarified policy elements, and consolidated all exceptions and waivers requirements.</p> <p>Section 1.5.4 – U.S. Citizen Exception Requests – Updated section to include policy elements:</p> <p>1.5.4.a – Persons of dual citizenship, where one of the citizenships includes U.S. Citizenship, shall be treated as U.S. Citizens for the purposes of this</p>

Version	Date	Description
		<p>directive.</p> <p>1.5.4.b – Additional compensating controls shall be maintained for foreign nationals, based on nations lists maintained by the DHS CSO.</p> <p>Section 1.6 – Information Sharing and Communication Strategy – Added policy element:</p> <p>1.6.a - For DHS purposes, electronic signatures are preferred to pen and ink or facsimile signatures in all cases except where pen & ink signatures are required by public law, Executive Order, or other agency requirements.</p> <p>Section 1.7 – Changes to Policy – Updated entire section</p> <p>Section 2.0 – Roles and Responsibilities – Reformats entire section. Places emphasis on DHS CISO and Component-level Information Security Roles. Secretary and senior management roles are moved to the end of the section. Some specific areas to note include:</p> <p>Section 2.1.1 – DHS Senior Agency Information Security Officer – Introduces this term and assigns duties to DHS CISO</p> <p>Section 2.1.2 – Chief Information Security Officer – Adds the following responsibilities:</p> <ul style="list-style-type: none"> - Appoint a DHS employee to serve as the Headquarters CISO - Appoint a DHS employee to serve as the National Security Systems (NSS) CISO <p>Section 2.1.3 – Component Chief Information Security Officer – Adds policy element:</p> <p>2.1.3.b - All Components shall be responsible to the appropriate CISO. Components without a fulltime CISO shall be responsible to the HQ CISO.</p> <p>Adds 4 additional CISOs to the list of Component CISOs:</p> <ul style="list-style-type: none"> Federal Law Enforcement Training Center Office of the Inspector General Headquarters, Department of Homeland Security The DHS CISO shall also appoint an NSS CISO <p>Section 2.1.4 – Component Information Systems Security Manager – Component CISO now works directly with the HQ CISO, rather than with the DHS CISO.</p> <p>Section 2.1.5 – Risk Executive – Introduces this term as per NIST.</p>

Version	Date	Description
		<p>Assigns responsibilities to CISOs (already performing these functions)</p> <p>Section 2.1.6 – Authorizing Official – Introduces this term as per NIST. Replaces the term Designated Approval Authority (DAA)</p> <p>Section 2.2.10 – DHS Employees, Contractors, and Vendors – Adds the requirement for vendors to follow DHS Information Security Policy</p> <p>Section 3.2 – Capital Planning and Investment Control – Adds policy element:</p> <p>3.2.f – Procurement authorities throughout DHS shall ensure that Homeland Security Acquisition Regulation (HSAR) provisions are fully enforced.</p> <p>Section 3.3 – Contractors and Outsourced Operations – Adds policy element:</p> <p>3.3.g – Procurement authorities throughout DHS shall ensure that Homeland Security Acquisition Regulation (HSAR) provisions are fully enforced.</p> <p>Section 3.5.2 – Contingency Planning – Updates and expands entire section.</p> <p>Section 3.5 – Configuration Management – Adds policy elements</p> <p>Section 3.7.f – If the information system uses operating systems or applications that do not have hardening or do not follow configuration guidance from the DHS CISO, the System Owner shall request an exception, including a proposed alternative secure configuration.</p> <p>Section 3.7.g – Components shall ensure that CM processes under their purview include and consider the results of a security impact analysis when considering proposed changes.</p> <p>Section 3.9 – Certification, Accreditation, and Security Assessments – Updates entire section</p> <p>Section 3.9.1 – FIPS Categorization and NIST SP 800-53 Controls – Removed table of controls and referred reader to Attachment M.</p> <p>Added Section 3.9.10 – Plan of Actions and Milestones and renumbered Sections 3.9.10-11 to 3.9.11-12</p> <p>Section 3.11.1 – CISO Council – Updates the term from CISO Board</p> <p>Section 3.14-3.14.6 – Privacy Sections – Updates all sections pertaining to privacy and privacy information, adds section 3.14.5 – Protecting Privacy Sensitive Systems</p> <p>Section 3.14.7 – E-Authentication – Renumbers this section from 3.14.6 (due to adding of privacy section 3.14.5)</p>

Version	Date	Description
		<p>Section 3.15 – DHS Chief Financial Officer Designated Systems – Section renamed from DHS Chief Financial Officer Designated Financial Systems</p> <p>Section 3.16 – Social Media – Added Social Media section to provide guidelines and address the Federal Government’s (including DHS) use of social media sites (You Tube, Twitter, etc)</p> <p>Section 4.1.2 – Rules of Behavior – Added policy element: 4.1.2.b – Components shall ensure that DHS users are trained regarding rules of behavior and that each user signs a copy prior to being granted user accounts or access to information systems or data.</p> <p>Section 4.1.5 – IT Security Awareness, Training, and Education – Updates entire section</p> <p>Section 4.1.6 – Separation from Duty – Updates policy element to require that all assets and data are recovered from departing individuals 4.1.6.b – Components shall establish procedures to ensure that all DHS information system-related property and assets are recovered from the departing individual and that sensitive information stored on any media is transferred to an authorized individual. Adds policy elements: 4.1.6.c - Accounts for personnel on extended absences shall be temporarily suspended. 4.1.6.d – System Owners shall review information system accounts supporting their programs at least annually.</p> <p>Section 4.3.2 – Media Marking and Transport – Adds “Transport” to section title and adds policy element: 4.3.2.b – Components shall control the transport of information system media containing sensitive data, outside of controlled areas and restrict the pickup, receipt, transfer, and delivery to authorized personnel.</p> <p>Section 4.6 – Wireless Network Communications – Updated section title from “Wireless Communication” and specifies “network communication” technologies in policy, rather than the more general “Wireless.” Removes references to the defunct “WMO.”</p> <p>Section 4.6.1 – Wireless Systems – Adds policy elements: 4.6.1.f – Component CISOs shall review all system applications for wireless usage, maintain an inventory of systems, and provide that inventory to the DHS CISO at least annually. 4.6.1.g – Component CISOs shall (i) establish usage restrictions and</p>

Version	Date	Description
		<p>implementation guidance for wireless technologies; and (ii) authorize, monitor, and control wireless access to DHS information systems.</p> <p>4.9.1 – Security Incidents and Incident Response and Reporting – Adds requirement for Components to maintain full SOC and CSIRC capability (May outsource to DHS SOC). Adds policy elements:</p> <p>4.9.1.k – Components shall maintain a full SOC and CSIRC capability or outsource this capability to the DHS SOC. The DHS SOC shall provide SOC and CSIRC services to Components in accordance with formal agreements. Information regarding incident response capability is available in Attachment F of the DHS 4300A Sensitive Systems Handbook.</p> <p>4.9.1.q – The DHS CISO shall publish Incident Response Testing and Exercise scenarios as required.</p> <p>4.9.1.r – The Component CISO for each Component providing an incident response capability shall ensure Incident Response Testing and Exercises are conducted annually in coordination with the DHS CISO.</p> <p>Section 5.1 – Identification and Authentication – Adds requirement for strong authentication following HSPD-12 implementation.</p> <p>5.1.f – Components shall implement strong authentication on servers, for system administrators and significant security personnel, within six (6) months of the Component’s implementation of HSPD-12.</p> <p>Section 5.4.1 – Remote Access and Dial-In – Updates section and adds policy element:</p> <p>5.4.1.f – The Public Switched Telephone Network (PSTN) shall not be connected to OneNet at any time.</p> <p>5.4.3 – Network Connectivity – Requires DHS CIO approval for all network connections outside of DHS. Also specifies requirement for CCB.</p> <p>5.4.3.g – The DHS CIO shall approve all interconnections between DHS information systems and non-DHS information systems. Components shall document interconnections with an ISA for each connection. The DHS CIO shall ensure that connections with other Federal Government Agencies are properly documented. A single ISA may be used for multiple connections provided that the security accreditation is the same for all connections covered by that ISA.</p> <p>5.4.3.1 - The appropriate CCB shall ensure that documentation associated with an approved change to an information system is updated to reflect the appropriate baseline. DHS systems that interface with OneNet shall also be subject to the OneNet CCB.</p> <p>Section 5.4.4 – Firewalls and Policy Enforcement Points – Updates language to include Policy Enforcement Points. Adds policy elements:</p>

Version	Date	Description
		<p>5.4.4.i – The DHS CISO shall establish policy to block or allow traffic sources and destinations at the DHS TIC PEPs. The DHS CISO policy will prevent traffic as directed by the DHS CIO.</p> <p>5.4.j – The DHS SOC shall oversee all enterprise PEPs.</p> <p>Section 5.4.5 – Internet Security – Prohibits Public Switched Telephone Network (PSTN) connection to OneNet.</p> <p>5.4.5.a – Any direct connection of OneNet, DHS networks, or DHS mission systems to the Internet or to extranets shall occur through DHS Trusted Internet Connection (TIC) PEPs. The PSTN shall not be connected to OneNet at any time.</p> <p>Section 5.5.3 – Public Key/Private Key – Assigns responsibility for non-human use of PKI to sponsors.</p> <p>5.5.3.g – Sponsors for non-human subscribers (organization, application, code-signing, or device) shall be responsible for the security of and use of the subscriber’s private keys. Every sponsor shall read, understand, and sign a “DHS PKI Subscriber Agreement for Sponsors” as a pre-condition for receiving certificates from a DHS CA for the non-human subscriber.</p> <p>Section 5.4.6 – Email Security – Prohibits auto-forwarding of DHS email to other than .gov addresses.</p> <p>5.4.6.i - Auto-forwarding or redirecting of DHS email to address outside of the .gov domain is prohibited and shall not be used. Users may manually forward individual messages after determining that the risk or consequences are low.</p> <p>Section 5.6 – Malware Protection – Updates term from “Virus.”</p>
7.1	September 30, 2009	<p>General Updates</p> <p>Standardized the term “IT system” to “information system”</p> <p>Standardized the term “DHS IT system” to “DHS information system”</p> <p>Updated the term “DHS Security Operations Center” to “DHS Enterprise Operations Center” and added definition in glossary</p> <p>Replaced “must” with “shall” in all policy statements</p> <p>Replaced “vendors” with “others working on behalf of DHS”</p> <p>Specific Updates</p> <p>Section 1.4.20 – Strong Authentication – Added definition for Strong Authentication</p> <p>Section 1.4.21 – Two-Factor Authentication – Added definition for Two-</p>

Version	Date	Description
		<p>Factor Authentication</p> <p>Section 2.2.4 – Component Chief Information Officer – Alleviated confusion regarding Component CIO responsibilities</p> <p>Section 2.2.5 – Chief Security Office – Removed erroneous CSO responsibilities which belong to Component CIOs</p> <p>Section 2.2.7 – DHS Chief Financial Officer – Updated policy elements to clarify applicable policies</p> <p>Section 3.1 – Basic Requirements (3.1.d, 3.1.g-j) – Updated policy elements to CISO/ISSM/ISSO responsibilities</p> <p>Section 3.7.f – Clarified Operating system exception requirements</p> <p>Section 3.9.1-m – Clarified requirements regarding TAF/RMS</p> <p>Section 3.15 – CFO Designated Systems – Major revisions to this section</p> <p>Section 4.2.6 and 5.4.1.a – Prohibits tethering to DHS devices</p> <p>Section 5.4.3.g-h – Clarifies interconnection and ISA approval</p> <p>Section 5.5 – Cryptography – Removed unnecessary elements from introductions and updated entire section with input from DHS PKI Steward</p>
7.2	June 21, 2010	<p>General Updates</p> <p>No general updates with this revision. Specific updates are listed below.</p> <p>Specific Updates</p> <p>Section 1.4.8 – Added FISMA language (transmits, stores, or processes data or information) to definition of DHS System</p> <p>Section 1.5.3.k – Removed requirement for Component Head to make recommendation regarding waivers; removed requirement to report <i>exceptions</i> on FISMA report.</p> <p>Section 2.1.6 – Adds requirement for AO to be a Federal employee</p> <p>Section 2.1.7 – Clarifies that CO is a senior management official; stipulates that CO must be a Federal employee</p> <p>Section 2.2.5 – Updated CSO role</p> <p>Section 3.2 – Added intro to CPIC section</p> <p>Section 3.5.2.h – Added requirement to coordinate CP and COOP testing moderate and high FIPS categorizations</p> <p>Section 3.15.a – Added requirement for CFO Designated Systems security assessments for key controls be tracked in TAF and adds requirement for tracking ST&E and SAR annually.</p>

Version	Date	Description
		<p>Section 3.15.c – Remaps control from RA-4 to RA-5</p> <p>Section 3.15.h – Adds mapping to IR-6</p> <p>Section 3.15.i – Remaps control from PL-3 to PL-2</p> <p>Section 3.17 – Added requirement to protect HIPPA information</p> <p>Section 3.9.8.1 – Clarifies the requirement for alternate sites for high availability systems</p> <p>Section 4.1.1.a – Added requirement for annual reviews of position sensitivity levels</p> <p>Section 4.1.1.c – Exempts active duty USCG and other personnel subject to UCMJ from background check requirements</p> <p>Section 4.1.4.c-d – Adds additional separation of duties requirements and restricts the use of administrator accounts</p> <p>Section 5.2.f – Limits the number of concurrent connections for FIPS-199 high systems</p> <p>Section 5.4.2.a – Limits network monitoring as per the Electronic Communications Act</p> <p>Section 5.4.3 – Added introduction to clarify ISA requirements</p> <p>Section 5.4.3.f – Clarifies the term “security policy” in context</p> <p>Section 5.4.3.m – Clarifies that the both AOs must accept risk for interconnected systems that do not require ISAs.</p> <p>Section 5.4.3.m-n – Adds stipulations to ISA requirements</p> <p>Section 5.5 – Updates language in entire section</p> <p>Section 5.5.3.j – Assigns the DHS PKI MA responsibility for maintaining Human Subscriber agreements</p>
7.2.1	August 9, 2010	<p>General Updates</p> <p>No general updates with this revision. Specific updates are listed below.</p> <p>Specific Updates</p> <p>Section 1.1 – Removes reference to 4300C; updates section to align with policy</p> <p>Section 1.4.1/3 – Updates Executive Order reference from 12958 to 13526</p> <p>Section 1.4.8 – Updates definition of DHS system to align with policy</p> <p>Section 1.4.17 – Updates the PII section</p> <p>Section 1.4.18 – Updates SPII section</p> <p>Section 1.5.3 – Adds requirement for Privacy Officer/PPOC approval for exceptions and waivers pertaining to Privacy Designated Systems</p> <p>Section 1.6.b/c – Requires installation and use of digital signatures and</p>

Version	Date	Description
		<p>certificates</p> <p>Section 2.1.6.d – Allows delegation of AO duty to review and approve administrators</p> <p>Section 2.2.6 – Updates DHS Chief Privacy Officer description</p> <p>Section 3.7.e – Adds requirement to include DHS certificate as part of FDCC</p> <p>Section 3.14 – Updates Privacy and Data Security section</p> <p>Section 3.14.1 – Updates PII section</p> <p>Section 3.14.2 – Updates PTA section</p> <p>Section 3.14.2.e – Updates impact level requirements for Privacy Sensitive Systems</p> <p>Section 3.14.3 – Updates PIA section</p> <p>Section 3.1.4.4 – Updates SORN section</p> <p>Section 3.14.4.a – Exempts SORN requirements</p> <p>Section 3.14.5 – Updates Privacy Sensitive Systems protection requirements</p> <p>Section 3.14.6.a – Updates privacy incident reporting requirements</p> <p>Section 3.14.7 – Updates privacy requirements for e-Auth</p> <p>Section 3.14.7.e – Adds PIA requirements for eAuth</p> <p>Section 4.1.1.e – Expands U.S. citizenship requirement for access to all DHS systems and networks</p> <p>Section 4.1.4.b – Allows delegation of AO duty to review and approve administrators</p> <p>Section 4.6.2.3.c – Clarifies prohibited use of SMS</p> <p>Section 4.8.4.h – Updates the term “trusted” to “cleared” maintenance personnel</p> <p>Section 4.12.i – Updates escort requirements for maintenance or disposal</p> <p>Section 4.12.j – Requires disabling of dial up on multifunction devices</p> <p>Section 5.4.3 – Clarifies definition of Network Connectivity</p> <p>Section 5.4.3.m/n – Clarifies requirement for ISA and aligns with policy</p> <p>Section 5.4.6.j – Requires DHS email systems to use a common naming convention</p> <p>Section 5.5.3.g – Prohibits sharing of personal private keys</p>
7.2.1.1	January 19, 2011	<p>General Updates</p> <p>No general updates with this revision. Specific updates are listed below.</p> <p>Specific Updates</p> <p>Section 4.8.1.a – Changes requirement for screensaver activation from five (5) to fifteen (15) minutes of inactivity.</p>

Version	Date	Description
9.1	July 24, 2012	<p>General Changes</p> <p>Style, grammar, and diction edited.</p> <p>Updated control references.</p> <p>Updated links.</p> <p>Replace “EOC” and “Emergency Operations Center” with “SOC” and “Security Operations Center” respectively.</p> <p>Replace “CSIRC” and “Computer Security Incident Response Center” with “SOC” and “Security Operations Center” respectively.</p> <p>Replace “certification and accreditation” and “C&A” with “security authorization process”.</p> <p>Replace “Certifying Official” with “Security Control Assessor”.</p> <p>Replace “ST&E Plan” with “security assessment plan”.</p> <p>Replace “ST&E” with “security control assessment”</p> <p>Replace “system security plan” with “security plan” and “SSP” with “SP”.</p> <p>Specific Updates:</p> <p>Section 1: Updated citations.</p> <p>Section 1.4.8.1: Change definition to specify that a GSS has only one ISSO.</p> <p>Section 1.4.8.2: Change definition to specify that an MA has only one ISSO.</p> <p>Section 1.5.1: Include language requiring waiver submissions to be coordinated with the AO.</p> <p>Section 1.5.2: Include language requiring waiver submissions to be coordinated with the AO.</p> <p>Section 1.5.3: Clarify language regarding submission of waivers and exceptions for CFO designated systems.</p> <p>Section 1.5.3.a: New policy element added to state that the 4300A Policy and Handbook apply to all DHS systems unless a waiver or exception has been granted.</p> <p>Section 1.6: Section 1.6, Information Sharing and Electronic Signature was divided into two sections – Section 1.6, Electronic Signatures, and Section 1.7, Information Sharing.</p> <p>Section 1.6.b: Changed to require use of electronic signatures where practicable.</p> <p>Section 1.6.d: Added new policy element, “DHS and Component systems shall be able to verify PIV credentials issued by other Federal agencies.”</p> <p>Section 1.6.e: Updated control reference.</p> <p>Section 1.8: Section 1.8, Threats, was added to the policy.</p> <p>Section 1.8.5: Section added defining <i>supply chain threat</i> and <i>supply chain</i>.</p> <p>Section 2.1.2: Add DHS CISO role as primary liaison to Component</p>

Version	Date	Description
		<p>officials, and to perform periodic compliance reviews for selected systems.</p> <p>Section 2.13: Update Component CISO duties and add to implement POA&M process and ensure that external providers who operate information systems meet the same security requirements as the Component.</p> <p>Include language to address the designation of a Deputy CISO by the Component CISO. Add two new responsibilities for Component CISO: Serve as principal advisor on information security matters; Report to the Component CIO on matters relating to the security of Component information Systems. Removed a lower bullet that these made redundant.</p> <p>Added Science and Technology (S&T) to the list of Components that shall have fulltime CISOs.</p> <p>NPPD added to the list of Components having a fulltime CISO.</p> <p>Section 2.1.4: Update list of Component ISSM duties and create a POA&M for each known vulnerability.</p> <p>Section 2.1.5: Add significantly expanded Risk Executive duties.</p> <p>Section 2.1.6: Add significantly expanded Authorizing Official duties.</p> <p>Section 2.1.6.a: Clarified language (designation of AOs at Department level).</p> <p>Section 2.1.6.b: Clarified language (designation of AOs at Component level).</p> <p>Section 2.1.8.g: New policy element added to ensure ISSO responsibility for responding to ICCB change request packages.</p> <p>Section 2.2.4: Includes new language stating that the Component CISO reports directly to the Component CIO.</p> <p>Section 2.2.8: Add Program Manager responsibility for POA&M content.</p> <p>Section 2.2.9: Add expanded System Owner duties.</p> <p>Section 2.2.10: Renumber previous version's Section 2.2.10 to be Section 2.2.11</p> <p>Section 2.2.10 [New]: Introduces and describes duties of Common Control Provider.</p> <p>Section 2.2.11: Renumbered from previous version's 2.2.10.</p> <p>Section 3.1.k: Added policy statement requiring SCAP compliance.</p> <p>Section 3.18: Section added containing Cloud Services policy.</p> <p>Section 3.2.g: Added new policy element, "Procurements for services and products involving facility or system access control shall be in accordance with the DHS guidance regarding HSPD-12 implementation."</p> <p>Section 3.5.2.c: Updated language to clarify requirements for backup policy and procedures.</p> <p>Section 3.5.2.f: Updated language to require table-top exercises for testing the CP for moderate availability systems.</p> <p>Section 3.7.f: Added new policy element, "Components shall monitor</p>

Version	Date	Description
		<p>USGCB (or DHS-approved USGCB variant) compliance using a NIST-validated Security Content Automation Protocol (SCAP) tool.”</p> <p>Section 3.9: Add requirement for Components to designate a Common Control Provider.</p> <p>Section 3.9.w: Policy element added to require common control catalogs for DHS enterprise services.</p> <p>Section 3.9.x: Policy element added to require the development of Enterprise System Security Agreements for enterprise services.</p> <p>Section 3.10.b: Policy element language was updated to clarify the function of information system security review and assistance programs.</p> <p>Section 3.11.3: Added section, including two policy statements, relative to Security Policy Working Group.</p> <p>Section 3.14.6.e: Updated reference title and hyperlink.</p> <p>Section 3.14.7.e: Policy element revised to require consultation with a privacy officer to determine if a change requires an updated PTA.</p> <p>Section 3.14.7.h: New policy element added to ensure that all new DHS information systems or those undergoing major upgrades shall use or support DHS PIV credentials</p> <p>Section 3.14: Language updated for readability.</p> <p>Section 3.14.4.c: Added new policy element, “Components shall review and republish SORNs every two (2) years as required by OMB A-130.”</p> <p>Section 3.14.7.f: Added new policy element, “Existing physical and logical access control systems shall be upgraded to use PIV credentials, in accordance with NIST and DHS guidelines.”</p> <p>Section 3.14.7.g: Added new policy element, “All new systems under development shall be enabled to use PIV credentials, in accordance with NIST and DHS guidelines, prior to being made operational.”</p> <p>Section 3.17: Added reference to NIST SP 800-66 for more information on HIPAA.</p> <p>Section 4.1.1.c: Includes new language to give Components the option to use background investigations completed by another Federal agency when granting system access to Federal employees.</p> <p>Section 4.1.1.c: Changed “Minimum Background Investigation (MBI)” to “Moderate Risk Background Investigation (MBI).”</p> <p>Section 4.1.1.d: Includes new language to give Components the option to use background investigations completed by another Federal agency when granting system access to contractor personnel.</p> <p>Section 4.1.4.d: Language updated to clarify usage of administrator accounts.</p> <p>Section 4.1.5.d: Policy element revised to clarify awareness training records requirements.</p> <p>Section 4.1.5.e: Policy element revised to clarify role-based training</p>

Version	Date	Description
		<p>records requirements.</p> <p>Section 4.1.5.f: Language updated to clarify requirements for security awareness training plan.</p> <p>Section 4.1.5.g: Policy element revised to require submission of an annual role-based training plan.</p> <p>Section 4.1.5.j: Policy element revised to require annual DHS CISO review of role-based training programs.</p> <p>Section 4.1.5.k: Policy element revised to require biannual submission of roster of significant information security personnel and to specify the standard information security roles.</p> <p>Section 4.3.1.b: Language updated to clarify protection of offsite backup media.</p> <p>Section 4.3.1.f: Policy element prohibiting connection of DHS removable media to non-DHS systems. It was already stated in 4.3.1.e.</p> <p>Section 4.5.4: Added reference to NIST SP 800-58 for more information on VoIP.</p> <p>Section 4.9.j: Language updated to require that Component SOCs report operationally to the respective Component CISO.</p> <p>Section 4.9.k: New policy element added, “The DHS EOC shall report operationally to the DHS CISO.”</p> <p>Section 4.9.1 [four.nine.ell]: Added policy statement requiring the NOC/SOC to be under the direction of a Government employee who shall be present at all times.</p> <p>Section 4.10: renumbered Section 4.9.1</p> <p>Section 4.10.1.1 renumbered to Section 4.9.1.1</p> <p>Section 4.10.1.2 renumbered to Section 4.9.1.2</p> <p>Section 4.10.1.3 renumbered to Section 4.9.1.3</p> <p>Section 4.10.1.4 renumbered to Section 4.9.1.4</p> <p>Section 4.10.1.5 renumbered to Section 4.9.1.5</p> <p>Section 4.10.1.6 renumbered to Section 4.9.1.6</p> <p>Section 4.10.2 renumbered to Section 4.9.2</p> <p>Section 4.10.3 renumbered to Section 4.9.3</p> <p>Section 4.11 renumbered to Section 4.10</p> <p>Section 4.12 renumbered to Section 4.11</p> <p>Section 4.13 renumbered to Section 4.12</p> <p>Section 4.9.1.b: Revised with clarification of reporting means and requirements.</p> <p>Section 4.9.1.c: Revised with clarification of reporting means and requirements.</p>

Version	Date	Description
		<p>Section 4.10: Revise list of annual system documentation updates.</p> <p>Section 4.11.c: Policy element replaced with new one stating that the policy applies “to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS data.”</p> <p>Section 4.11.c: Policy element was moved to 1.5.3.a.</p> <p>Section 4.12.d: Updated control reference.</p> <p>Section 4.11</p> <p>Section 4.10.c: Updated control reference.</p> <p>Section 5.1.g: Policy element added to require use of PIV credentials for logical authentication where available.</p> <p>Section 5.2.b: Updated control reference.</p> <p>Section 5.2.e: Updated control reference.</p> <p>Section 5.2.f: Policy element revised to allow concurrent sessions to one if strong authentication is used.</p> <p>Section 5.2.g: New policy element added to ensure preservation of identification and access requirements for all data-at-rest.</p> <p>Section 5.4.1.a: Updated control reference.</p> <p>Section 5.4.4.b: Updated control reference.</p> <p>Section 5.4.1.e: Policy element removed.</p> <p>Section 5.4.1.f: Policy element removed.</p> <p>Section 5.4.6.k: Added policy statement moved from 5.4.7.b.</p> <p>Section 5.4.7.b: Deleted and becomes new policy statement 5.4.6.k.</p> <p>Section 5.5.2: Revised to address the two DHS PKIs now functioning: DHS FPKI and DHS Internal NPE PKI.</p> <p>Section 5.5.3: Revised to address the two DHS PKIs now functioning: DHS FPKI and DHS Internal NPE PKI.</p> <p>Section 5.7.e: Updated control reference.</p> <p>Section 5.8: Added new section, including two policy statements, relative to IT supply chain risks and protection against supply chain threats.</p> <p>Appendix A: Included new acronyms</p> <p>Appendix B: Revised definition of Accreditation Package to reflect new list of documentation.</p> <p>Appendix C: Updated references</p>