DHS Sensitive Systems Policy Directive 4300A

Version 12.01
February 12, 2016

This Policy implements DHS Management Directive 140-01
"Information Technology System Security," July 31, 2007

Protecting the Information that Secures the Homeland

This page intentionally left blank

FOREWORD

The Department of Homeland Security (DHS) 4300 series of information security publications are the official documents that articulate Departmental policies, standards, and guidelines in accordance with DHS Management Directive 140-01 *Information Technology System Security*.

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

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

JEFFREY L EISENSMITH

Digitally signed by JEFFREY L EISENSMITH
DN: c=US, o=U.S. Government, ou=Department of Homeland Security, ou=DHS HQ, ou=People, cn=JEFFREY L EISENSMITH, 0.9.2342.19200300.100.1.1=0387904707.DHS HQ.1
Date: 2016.05.20 11:21:59 -04'00'

/S/

Jeffrey Eisensmith
Chief Information Security Officer
Department of Homeland Security

This page intentionally left blank

TABLE OF CONTENTS

1.0 INTRODUCTION....1
1.1 Information Security Program....1
1.2 Authorities....2
1.3 Policy Overview....2
1.4 Definitions....3
1.4.1 Classified National Security Information....3
1.4.2 Component....3
1.4.3 Continuity of Operations....3
1.4.4 Continuity of Operations Plan (COOP)....3
1.4.5 DHS System....4
1.4.6 Essential Functions....4
1.4.7 Federal Information Security Modernization Act (FISMA)....4
1.4.8 Foreign Intelligence Information....4
1.4.9 General Support System....4
1.4.10 Information Technology....5
1.4.11 Major Application....5
1.4.12 National Intelligence Information....5
1.4.13 Operational Data....6
1.4.14 Personally Identifiable Information....6
1.4.15 Privacy Sensitive System....6
1.4.16 Privileged User....6
1.4.17 Public Information....6
1.4.18 Sensitive Information....6
1.4.19 Sensitive Personally Identifiable Information (SPII)....6
1.4.20 Sensitive System....7
1.4.21 Strong Authentication....7
1.4.22 Trust Zone....7
1.4.23 Two-Factor Authentication....7
1.4.24 Visitor....7
1.4.25 Vital Records....8
1.5 Waivers....8
1.5.1 Waiver Requests....8
1.5.2 Requests for Exception to U.S. Citizenship Requirement....10
1.6 Digital and Other Electronic Signatures....11
1.6.1 Digital Signatures and Other Electronic Signature Methods....11
1.6.2 Digital Signatures....14
1.7 Information Sharing....19
1.8 Threats....20
1.8.1 Insider Threats....20
1.8.2 Criminal Threats....21
1.8.3 Foreign Threats....21
1.8.4 Lost or Stolen Equipment....21
1.8.5 Supply Chain Threats....21
1.9 Changes to Policy....22

2.0 ROLES AND RESPONSIBILITIES 23
2.1 Information Security Program Roles 23
2.1.1 DHS Senior Agency Information Security Officer 23
2.1.2 DHS Chief Information Security Officer 24
2.1.3 Component Chief Information Security Officer 26
2.1.4 Component Information Systems Security Manager 29
2.1.5 Risk Executive 30
2.1.6 Authorizing Official 31
2.1.7 Security Control Assessor 32
2.1.8 Information Systems Security Officer 33
2.1.9 Ongoing Authorization Manager and Operational Risk Management Board 34
2.1.10 DHS Security Operations Center 35
2.1.11 DHS Component Security Operations Centers 36
2.2 Other Roles 37
2.2.1 Secretary of Homeland Security 37
2.2.2 Under Secretaries and Heads of DHS Components 38
2.2.3 DHS Chief Information Officer 39
2.2.4 Component Chief Information Officer 40
2.2.5 DHS Chief Security Officer 42
2.2.6 DHS Chief Privacy Officer 42
2.2.7 DHS Chief Financial Officer 44
2.2.8 Program Managers 45
2.2.9 System Owners 45
2.2.10 Common Control Provider 46
2.2.11 DHS Employees, Contractors, and Others Working on Behalf of DHS 47

3.0 MANAGEMENT POLICIES 48
3.1 Basic Requirements 48
3.2 Capital Planning and Investment Control 49
3.3 Contractors and Outsourced Operations 50
3.4 Performance Measures and Metrics 52
3.5 Continuity Planning for Critical DHS Assets 52
3.5.1 Continuity of Operations Planning 52
3.5.2 Contingency Planning 53
3.6 Systems Engineering Life Cycle 55
3.7 Configuration Management 55
3.8 Risk Management 57
3.9 Security Authorization and Security Control Assessments 58
3.9.1 Ongoing Authorization 61
3.10 Information Security Review and Assistance 63
3.11 Security Working Groups and Forums 63
3.11.1 CISO Council 63
3.11.2 DHS Information Security Training Working Group 64
3.11.3 DHS Security Policy Working Group 65
3.11.4 DHS Enterprise Services Security Working Group 65

3.12 Information Security Policy Violation and Disciplinary Action 65
3.13 Required Reporting 66
3.14 Privacy and Data Security 66
3.14.1 Personally Identifiable Information 67
3.14.2 Privacy Threshold Analyses 70
3.14.3 Privacy Impact Assessments 70
3.14.4 System of Records Notices 72
3.14.5 Protecting Privacy Sensitive Systems 74
3.14.6 Privacy Incident Reporting 75
3.14.7 E-Authentication 76
3.14.8 Use Limitation and External Information Sharing 77
3.15 DHS CFO Designated Systems 78
3.16 Social Media 80
3.17 Health Insurance Portability and Accountability Act 81
3.18 Cloud Services 83

4.0 OPERATIONAL POLICIES 84
4.1 Personnel 84
4.1.1 Citizenship, Personnel Screening, and Position Categorization 85
4.1.2 Rules of Behavior 86
4.1.3 Access to Sensitive Information 86
4.1.4 Segregation of Duties and Least Privilege 86
4.1.5 Information Security and Privacy Awareness, Training, and Education 87
4.1.6 Separation from Duty 89
4.2 Physical Security 89
4.2.1 General Physical Access 89
4.2.2 Sensitive Facility 91
4.3 Media Controls 92
4.3.1 Media Protection 92
4.3.2 Media Marking and Transport 93
4.3.3 Media Sanitization and Disposal 93
4.3.4 Production, Input/Output Controls 93
4.4 Voice Communications Security 94
4.4.1 Private Branch Exchange 94
4.4.2 Telephone Communications 94
4.4.3 Voice Mail 94
4.5 Data Communications 94
4.5.1 Telecommunications Protection Techniques 94
4.5.2 Facsimiles 95
4.5.3 Video Teleconferencing 95
4.5.4 Voice over Data Networks 96
4.6 Wireless Network Communications 96
4.6.1 Wireless Systems 97
4.6.2 Wireless Mobile Devices 98
4.6.2.1 Cellular Phones 101
4.6.2.2 Pagers 102

4.6.2.3 Multifunctional Wireless Devices 102
4.6.2.4 Bluetooth 102
4.6.3 Wireless Tactical Systems 103
4.6.4 Radio Frequency Identification....104
4.7 Overseas Communications....105
4.8 Equipment 105
4.8.1 Workstations 105
4.8.2 Laptop Computers and Other Mobile Computing Devices 106
4.8.3 Personally Owned Equipment and Software 106
4.8.4 Hardware and Software....108
4.8.5 Personal Use of Government Office Equipment and DHS Systems/Computers....109
4.8.6 Wireless Settings for Peripheral Equipment 111
4.9 Department Information Security Operations....111
4.9.1 Security Incidents and Incident Response and Reporting....113
4.9.2 Law Enforcement Incident Response 115
4.10 Documentation 115
4.11 Information and Data Backup 116
4.12 Converging Technologies 117

5.0 TECHNICAL POLICIES 119
5.1 Identification and Authentication 119
5.1.1 Passwords....120
5.2 Access Control 122
5.2.1 Automatic Account Lockout....122
5.2.2 Automatic Session Termination....123
5.2.3 Warning Banner 123
5.3 Auditing 124
5.4 Network and Communications Security 125
5.4.1 Remote Access and Dial-In 125
5.4.2 Network Security Monitoring 126
5.4.3 Network Connectivity....127
5.4.4 Firewalls and Policy Enforcement Points 129
5.4.5 Internet Security....131
5.4.6 Email Security....132
5.4.7 Personal Email Accounts 133
5.4.8 Testing and Vulnerability Management....134
5.4.9 Peer-to-Peer Technology 135
5.5 Cryptography 135
5.5.1 Encryption....135
5.5.2 Public Key Infrastructure 135
5.5.3 Public Key/Private Key....144
5.6 Malware Protection 146
5.7 Product Assurance 147
5.8 Supply Chain....148
5.8.1 Business Impact 148

5.8.2 Supply Chain Risk Management Plans 149
6.0 DOCUMENT CHANGE REQUESTS 150
7.0 QUESTIONS AND COMMENTS 150
APPENDIX A ACRONYMS AND ABBREVIATIONS 151
APPENDIX B GLOSSARY 159
APPENDIX C REFERENCES 167
APPENDIX D DOCUMENT CHANGE HISTORY 171

1.0 INTRODUCTION

This document articulates the Department of Homeland Security (DHS) Information Security Program policies for sensitive systems. Procedures for implementing these policies are outlined in a companion publication, *DHS 4300A Sensitive Systems Handbook*. This Policy Directive and the *Handbook* serve as the foundation on which Components are to develop and implement their own information security programs. The Baseline Security Requirements (BLSR) included in the Handbook must be addressed when developing and maintaining information security documents.

1.1 Information Security Program

The DHS Information Security Program provides a baseline of policies, procedures, standards, and guidelines for DHS Components. This Policy Directive provides direction to managers and senior executives for managing and protecting sensitive systems. It also defines policies relating to management, operational, and technical controls necessary for ensuring confidentiality, integrity, availability, authenticity, and nonrepudiation in DHS information system infrastructure and operations. The policy elements expressed in this Policy Directive are designed to be broad in scope to accommodate the diverse DHS operating environments. Each Component or Office is responsible for identifying, developing, and implementing any additional policies needed to meet their specific requirements. Implementation information can often be found in specific National Institute of Standards and Technology (NIST) publications, such as NIST Special Publication (SP) 800-53, Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations."

This Policy Directive pertains to DHS Sensitive Systems, as distinct from DHS National Security Systems (NSS), which are governed by DHS National Security Systems Policy Directive 4300B series, available on the DHS Chief Information Security Officer (CISO) Web site. The 4300B series applies to all DHS elements, employees, contractors, detailees, others working on behalf of DHS, and users of DHS NSS that collect, generate, process, store, display, transmit, or receive Confidential, Secret, or Top Secret classified national security information.

Policy elements are effective when issued. Failure to implement any policy element within 135 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 DHS Chief Information Security Officer (CISO) will ensure that appropriate tool changes are made available to the Department within 90 days of the changes.

1.2 Authorities

The following are authoritative references for the DHS Sensitive Information Security Program. Additional references are located in Appendix C to this Policy Directive.

- E-Government Act of 2002, Public Law 107–347, 116 Stat. 2899, 44 U.S.C. 101
- Federal Information SecurityModernization Act of 2014 (FISMA), Public Law 113-283; 128 Stat 3073
- Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Transmittal Memorandum 4, 2010
- DHS Management Directive MD 140-01, "Information Technology Systems Security," July 31, 2007
- National Institute of Standards and Technology (NIST) Federal Information Processing Standard FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006
- NIST Special Publication (SP) 800-53, Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013, with updates as of January 22, 2015
- NIST SP 800-37, Rev 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 2010

1.3 Policy Overview

DHS information security policies define the security management structure and foundation needed to ensure adequate control over DHS sensitive information and systems. 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 the people responsible for use of the system. 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 are the security controls executed by the 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.

DHS privacy controls have been added to DHS information security policy documents to comply with the publication of NIST SP 800-53, Rev.4, Appendix J: "Privacy Control Catalog." The privacy controls focus on ensuring information privacy, distinct from, but closely related to information security. Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of Personally Identifiable Information (PII).

1.4 Definitions

The definitions in this section apply to the policies and procedures discussed in this document. In general, the sources for the definitions given in this Section are relevant NIST documents. Other definitions may be found in Committee on National Security Systems (CNSS) Instruction No. 4009, "National Information Assurance Glossary," 26 April 2010. Definitions bearing on Privacy are sourced from *Privacy Incident Handling Guidance* and the *Privacy Compliance* documentation issued by the DHS Privacy Office.

1.4.1 Classified National Security Information

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

1.4.2 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's, Counselors, and staff, when approved as such by the Secretary), including both Operational Components and Support Components (also known as Headquarters Components). [Source *DHS Lexicon* and DHS Management Directive 112-01]

1.4.3 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 of office and the emergency delegation of authority
- Provide for the safekeeping of vital records and databases
- Identify alternate operating facilities, if necessary
- Provide for interoperable communications
- Validate the capability to recover through tests, training, and exercises

1.4.4 Continuity of Operations Plan (COOP)

A predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations. [Source NIST SP 800-34]

1.4.5 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*.

1.4.6 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.

1.4.7 Federal Information Security Modernization Act (FISMA)

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.

FISMA requires that the Chief Information Officer (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

1.4.8 Foreign Intelligence Information

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

1.4.9 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 GSSs include local area networks (LAN), including smart terminals that support a

branch office, Department-wide backbones, communications networks, and Departmental data processing centers including their operating systems and utilities.

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 SOC. Every GSS must have an Information Systems Security Officer (ISSO) assigned.

1.4.10 Information Technology

Division E of the Clinger-Cohen Actof 1996 (Public Law 104-106) 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"

For purposes of the preceding definition, "equipment" refers to that used by any DHS office, 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 *information technology system*.

1.4.11 Major Application

A *major application* (MA) is an automated information system (AIS) that OMB Circular A-130 defines as requiring "…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."

All Federal applications require some level of protection. Certain applications, because of the information they contain, however, require special management oversight and should be classified 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.

1.4.12 National Intelligence Information

The Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458, 118 Stat. 3662) amended the National Security Act of 1947 (50 U.S.C. 401a) to provide the following definition:

> ''(5) 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.''.

1.4.13 Operational Data

Operational data is information used in any DHS mission activity.

1.4.14 Personally Identifiable Information

Personally Identifiable Information (PII)" means information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual regardless of whether the individual is a United States citizen, legal permanent resident, or a visitor to the United States. [see also Sensitive Personally Identifiable Information (SPII)]

1.4.15 Privacy Sensitive System

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

1.4.16 Privileged User

A *privileged user* is a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. (Source: NISTIR 7298 rev 2.0

1.4.17 Public Information

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

1.4.18 Sensitive Information

Sensitive Information is any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy of individuals, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy.

Sensitive Information includes:

- Chemical-terrorism Vulnerability Information (CVI)
- Protected Critical Infrastructure Information (PCII)
- Sensitive Security Information (SSI)
- Personally Identifiable Information (PII)

1.4.19 Sensitive Personally Identifiable Information (SPII)

Sensitive Personally Identifiable Information (SPII) is a subset of PII [see definition above], which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements..

1.4.20 Sensitive System

A *sensitive system* is any combination of facilities, equipment, personnel, procedures, and communications that is integrated for a specific purpose, and that may be vulnerable to an adversarial attack by an adversary seeking to violate or disrupt the system's confidentiality, integrity, or availability.

1.4.21 Strong Authentication

Strong authentication is a method used to secure computer systems and/or networks by verifying a user's identity by requiring two-factors in order to authenticate (something you know, something you are, or something you have). Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. [See the discussion of Level 4 assurance in NIST SP 800-63-2, "Electronic Authentication Guideline," (August 2013)]

1.4.22 Trust Zone

A *Trust Zone* consists of any combination of people, information resources, IT 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.

1.4.23 Two-Factor Authentication

The classic paradigm for authentication systems identifies three factors as the cornerstone of authentication:

- *Something you know* (for example, a password or Personal Identification Number (PIN)
- *Something you have* (for example, an ID badge or a cryptographic key)
- *Something you are* (for example, a fingerprint or other biometric data)

The strength of authentication systems is largely determined by the number of factors incorporated by the system. Implementations that use two factors are considered to be stronger than those that use only one factor." A requirement for two of the three factors listed above constitutes two factor authentication.

1.4.24 Visitor

A guest or temporary employee who presents themselves or is presented by a sponsor, for entry for less than 6 months to a secured facility that is not their primary work location. (Source: DHS Lexicon)

The visitor is placed in one of two categorizes, either ***escort required*** or ***no escort required***. ***Escort required*** visitors are escorted at all times. ***No escort required*** visitors are granted limited general access to the facility without an escort. Escort procedures for classified areas are indicated in Management Directive 11051 "SCIF Escort Procedures." (Source: DHS Lexicon)

1.4.25 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 Order (EO).

1.5 Waivers

When a Component is unable to fully comply with any portion of this Policy Directive, it may request a waiver. Waiver requests should be 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 12 months, the Component must submit a waiver request to the DHS CISO. If the material weakness exists in a financial system, the Component Chief Financial Officer (CFO) must also approve the waiver request before sending to the DHS CISO. If the material weakness exists in a system processing PII, the Component Privacy Officer or Privacy Point of Contact (PPOC) and DHS Chief Privacy Officer must also approve the waiver request before sending to the DHS CISO.

An approved waiver does not bring the system into compliance with policy; it is an acknowledgement by the DHS CISO of the system's non-compliance with policy and that an acceptable plan to remediate the weakness has been provided and compensating controls have been implemented.

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

1.5.1 Waiver Requests

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

Component ISSOs, audit liaisons, and others may develop the waiver request, but the System Owner shall submit the request through the Component's CISO/ISSM. All submitters shall coordinate with the Authorizing Official (AO) prior to submission

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

Additionally, any waiver requests for financial systems must be submitted to and approved by the Component's CFO prior to submission to the DHS CISO. Any waiver request for sensitive systems with PII information must be submitted to and approved by the Component's Privacy Officer or senior PPOC prior to being submitted to the DHS CISO.

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

Policy ID	DHS Policy Statements	Relevant Controls
1.5.1.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 information unless an approved waiver has been granted. This includes prototypes, telecommunications systems, and all systems in all phases of the Systems Engineering Life Cycle (SELC).	SA-3
1.5.1.b	Systems not yet authorized to operate when this policy is issued shall comply with all of its policy statements or obtain appropriate waivers. Systems with an Authority to Operate (ATO) shall comply within 135 days of the date of this Policy is issued or obtain appropriate waivers. (A new ATO is only required for significant changes.)	PL-1
1.5.1.c	Components shall request a waiver whenever they are unable to comply fully with any portion of this policy.	CA-2
1.5.1.d	The Component CISO/ISSM shall approve all waiver requests prior to submitting them to the DHS CISO.	CA-6
1.5.1.e	The Component CIO shall approve any waiver request that results in a total waiver time exceeding (12 months before sending the request to the DHS CISO.	---
1.5.1.f	The Component CFO shall approve all requests for waivers for financial systems prior to their submission to the DHS CISO.	CA-6
1.5.1.g	The Component's Privacy Officer or Senior PPOC shall approve all requests for waivers for sensitive systems processing PII or SPII prior to their submission to the DHS CISO.	---

Policy ID	DHS Policy Statements	Relevant Controls
1.5.1.h	The DHS Chief Privacy Officer shall approve all requests for waivers for compliance with any privacy control in Appendix J of NIST SP 800-53 prior to their submission to the DHS CISO.	---

1.5.2 Requests for Exception to U.S. Citizenship Requirement

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

Policy ID	DHS Policy Statements	Relevant Controls
1.5.2.a	Any Person of dual-citizenship (one being a US citizenship) and any Legal Permanent Resident who requires access to DHS systems as a validated representative of foreign power shall be processed as indicated in Section 1.5.2.	---
1.5.2.b	Exceptions to the U.S. Citizenship requirement shall be requested by submitting a completed Foreign National Visitor Access Request form to the DHS Office of the OCSO for each foreign national requiring access to DHS systems and networks.	PS-3
1.5.2.c	Component CISOs shall select a Foreign Access Coordinator to be the point of contact to the DHS OCSO for processing requests for exception to the U.S. Citizenship policy requirement (4.1.1.e). The Component shall notify OCSO of the selected Foreign Access Coordinator.	--
1.5.2.d	Foreign Access Coordinators shall, in coordination with the DHS OCSO, conduct an assessment of the risk of granting access to DHS systems by the Foreign National-specified and provide a recommendation to the Component CISO regarding the approval or disapproval of the request.	--

1.6 Digital and Other Electronic Signatures

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" 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.

Please refer to the "DHS Electronic Signature Policy Guidance" document for guidance on electronic signature policy

1.6.1 Digital Signatures and Other Electronic Signature Methods

The following DHS Policy Statements are applicable to both digital signatures and other electronic signature methods.

Policy ID	DHS Policy Statements	Relevant Controls
1.6.1.a	Digital signatures or other electronic signature methods shall be used whenever practical, except where handwritten signatures are required by law, regulation, Executive Order, or other agency requirement. Digital signature or other electronic signature methods, when properly executed, shall be accepted to the maximum extent practicable.	---
1.6.1.b	Electronic signatures, including digital signatures, shall be implemented by applications with the necessary security controls and practices such that: 1) the signer cannot successfully repudiate that he/she intended to sign, or that he/she applied the electronic signature; and 2) the integrity of the signed content cannot be successfully challenged.	---

Policy ID	DHS Policy Statements	Relevant Controls
1.6.1.c	When a signature is required on electronic documents, transactions, communications, etc. for use within DHS, or for use for intra-governmental transactions, communications, etc., where all potential signers possess a Personal Identity Verification (PIV) card, Department of Defense (DOD)-issued Common Access Card (CAC), or PIV-I card (and the associated card readers, software, and verification processes are in place), the signing process shall employ a digital signature created by a properly identified signer through the use of their PIV card, CAC issued by DOD, or PIV-I card, whenever possible. Signers may use their software-based digital signature certificate that meets the requirements specified in Section 1.6.2.a below for signing when their PIV card, DOD-issued CAC, or PIV-I card cannot be used. Other electronic signature methods may be used when it is determined that it is not possible for the signer to use his/her PIV card, DOD-issued CAC, PIV-I card, or software-based digital signature certificate that meets the requirements specified in Section 1.6.2.a below. For legally binding signatures, the determination of what other electronic signature method shall be used must be based on a risk assessment of the likelihood of a successful challenge to the enforceability of the signature, and the monetary loss, or other adverse impact of an unenforceable signature.	---
1.6.1.d	The following requirements shall be met when implementing legally binding signatures using Digital Signature or an Other Electronic Signature Method: 1) The Signer must use an acceptable electronic form of signature; 2) The electronic form of signature must be executed or adopted by a person with the intent to sign the electronic record; 3) The electronic form of signature must be attached to or associated with the electronic record being signed; 4) There must be a means to identify and authenticate a particular person as the signer; and 5) There must be a means to preserve the integrity of the signed record.	---
1.6.1.e	When implementing one or more legally binding Digital Signatures in an electronic document, transaction, communication, etc., and the intent to sign for each signature is not evidenced by the context of the content being signed, a clear and conspicuous notice shall be incorporated into that electronic document, transaction, communication, etc., just prior to the location each signature, that indicates: 1) That an electronic signature is being created, and what constitutes the execution of the signature, 2) The reason for signing (for that specific signature), and 3) That when completed, it will constitute the Signer's legally binding signature.	---

Policy ID	DHS Policy Statements	Relevant Controls
1.6.1.f	When implementing legally binding electronic signatures for a specific use, where Other Electronic Signature Methods will be used, the risk assessment process, described in the "DHS Electronic Signature Policy Guidance" document, Section I.G. "Determining Which Electronic Signature Method to Use - Risk Assessment and Cost-Benefit Analysis", shall be used to determine the overall level of risk, and the specific approaches to be implemented to meet each of the following five requirements for legally binding signatures: 1) The Signer must use an acceptable electronic form of signature; 2) The electronic form of signature must be executed or adopted by a person with the intent to sign the electronic record; 3) The electronic form of signature must be attached to or associated with the electronic record being signed; 4) There must be a means to identify and authenticate a particular person as the signer; 5) There must be a means to preserve the integrity of the signed record.	---
1.6.1.g	The date and time a legally binding signature is executed, using Digital Signature or an Other Electronic Signature Method, shall be captured and incorporated as part of the record of the signature. The captured date and time must be accurate and trustworthy. Within DHS, legally binding signatures using a digital signature or other electronic signature method shall be executed on systems whose system clocks have been synchronized via Network Time Protocol (NTP) with DHS networks, and are managed to prevent unauthorized changes to the system clock. When the signature is executed, the date and time from the system clock shall be captured and incorporated as part of the record of the signature. When a legally binding signature must be executed on a system whose system clock is not synchronized via NTP and not managed to prevent unauthorized changes to the system clock, the signer is responsible for ensuring that the date and time incorporated as part of the record of the signature is accurate.	---
1.6.1.h	The visual context of an electronic signature implemented using digital signature or other electronic signature method, shall be maintained. The Relying Parties for the electronically signed document, transaction, communication, etc. must be able to view the exact format and content of the document, transaction, communication, etc. that the Signer saw when he or she signed it.	---

Policy ID	DHS Policy Statements	Relevant Controls
1.6.1.i	Where a DHS entity is the Relying Party for an electronic signature executed on a non-DHS system by an external signer, using a digital signature or other electronic signature method, the DHS entity shall determine whether the asserted signing date and time is sufficiently accurate and trustworthy to be acceptable for the intended use of the signature.	---
1.6.1.j	Electronically signed records shall be maintained based on operational needs, perception of risks, and historical value, as formalized through corresponding Records Disposition Schedules approved by the National Archives and Records Administration (NARA). Operational needs shall be determined on the basis of the approach taken to ensure the availability, accessibility, and trustworthiness of electronically signed records over time.	---
1.6.1. k	The Component CISO shall approve the design, development, resources and infrastructure for implementations of electronic signatures using Digital Signatures or Other Electronic Signature Methods. The adoption and integration of legally binding electronic signature capabilities into workflows, business processes, specific document types, etc., shall be reviewed and approved by the Component General Counsel and by the Component Chief Records Officer. Additional review/endorsement by other cognizant officials (e.g., Privacy Officer; Chief Financial Officer; Forms Management Officer; etc.) shall be obtained when appropriate.	---
1.6.1.l	All implementations of digital signatures or other electronic signature methods in DHS shall comply with the requirements of DHS Sensitive Systems Policy Directive 4300A. Existing (legacy) implementations of electronic signatures shall be brought into compliance with DHS Sensitive Systems Policy Directive 4300A as soon as is practical, but in no case later than 12 months, or a waiver must be obtained. The waiver shall be requested in writing and submitted to the DHS CISO.	---

1.6.2 Digital Signatures

The following policy statements are applicable only to digital signatures.

<table>
<tr><th>Policy ID</th><th>DHS Policy Statements</th><th>Relevant Controls</th></tr>
<tr><td>1.6.2.a</td><td>Digital signatures shall not be accepted unless the following conditions are met:
1) Standard Path Development and Validation (PDVAL) software verifies the validity of the signer's signature verification certificate as of the time the signature was executed; and
2) The certificate is authorized for signature use (i.e., has the digital signature and non-repudiation key usage bits set in the keyUsage extension); and
3) The certificate was;
i) Issued by DHS Principal Certification Authority (CA) (DHS CA4) under one of the following U.S. Common Policy Framework certificate policies,
<table>
<tr><th>Policy</th><th>Policy Object Identifier</th></tr>
<tr><td>id-fpki-common-policy</td><td>::= {2 16 840 1 101 3 2 1 3 6}</td></tr>
<tr><td>id-fpki-common-hardware</td><td>::= {2 16 840 1 101 3 2 1 3 7}</td></tr>
<tr><td>id-fpki-common-High</td><td>::= {2 16 840 1 101 3 2 1 3 16}</td></tr>
</table>
as indicated by the Policy Object Identifier (OID) entered in the Certificate Policies extension in the certificate; or
ii) Issued by another U.S. Federal Government (CA that is subordinate to the U.S. Common Root CA under one of the following U.S. Common Policy Framework certificate policies,
<table>
<tr><th>Policy</th><th>Policy Object Identifier</th></tr>
<tr><td>id-fpki-common-policy</td><td>::= {2 16 840 1 101 3 2 1 3 6}</td></tr>
<tr><td>id-fpki-common-hardware</td><td>::= {2 16 840 1 101 3 2 1 3 7}</td></tr>
<tr><td>id-fpki-common-High</td><td>::= {2 16 840 1 101 3 2 1 3 16}</td></tr>
</table>
as indicated by the Policy OID entered in the Certificate Policies extension in the certificate; or
iii) Issued by a CA from another PKI cross-certified with the Federal Bridge Certification Authority (FBCA), where the certificate is issued under a certificate policy that maps to one of the following FBCA certificate policies,</td><td>---</td></tr>
</table>

<table>
<tr><th>Policy ID</th><th>DHS Policy Statements</th><th>Relevant Controls</th></tr>
<tr><td></td><td>
<table>
<tr><th>Policy</th><th>Policy Object Identifier</th></tr>
<tr><td>id-fpki-certpcy-mediumAssurance</td><td>::= { 2 16 840 1 101 3 2 1 3 3 }</td></tr>
<tr><td>id-fpki-certpcy-mediumHardware</td><td>::= { 2 16 840 1 101 3 2 1 3 12 }</td></tr>
<tr><td>id-fpki-certpcy-highAssurance</td><td>::= { 2 16 840 1 101 3 2 1 3 4 }</td></tr>
<tr><td>id-fpki-certpcy-pivi-hardware</td><td>::= { 2 16 840 1 101 3 2 1 3 18 }</td></tr>
</table>
as indicated by the PolicyMappings extension in the cross-certificate issued by the FBCA to the Root CA for the Signer's PKI, mapping an appropriate FBCA policy OID from the table above to the policy OID in the Certificate Policies extension from the Signer's certificate.
</td><td></td></tr>
<tr><td>1.6.2.b</td><td>If a digital signature is time stamped by a Trusted Timestamp Authority approved by the DHS CISO, DHS relying parties for the signature shall accept the time stamp as a trustworthy indicator that the digital signature was executed prior to that time.</td><td>---</td></tr>
<tr><td>1.6.2.c</td><td>For electronic documents, transactions, communications, etc. containing legally binding digital signatures, a visible signature block containing information about the signer and the signature shall be embedded for each signature, when possible. The visible signature block for each signature shall be located in proximity to, but after the statement in the document, transaction, communications, etc. indicating the intent of that signature.

The visible signature block shall be formatted to clearly indicate that it is a block of information about the signature, and shall contain:

1) The name of the signer (mandatory)
2) The Role of the signer (mandatory)
3) The date and time the signature was executed (mandatory)
4) A graphical depiction or image of the signer's handwritten signature (recommended)
5) Additional information as appropriate (optional)

The presence of a visual signature block shall not be used to indicate that a digital signature has been validated. A relying party must validate a digital signature using standard Path Development and Validation (PDVAL) protocols each time they make a determination to trust on not trust the digital signature.</td><td>---</td></tr>
<tr><td>1.6.2.d</td><td>Since any change to a digitally signed record will prevent validation of the digital signature, the use of stable file formats, with broad product support for</td><td>---</td></tr>
</table>

Policy ID	DHS Policy Statements	Relevant Controls
	backwards compatibility is essential to maintaining digitally signed records. Electronic documents, transactions, communications, etc. to be digitally signed shall be limited to file formats that will be stable over the retention period of the signed record. Suggested stable standard file formats include, but are not limited to: 1) American Standard Code for Information Exchange (ASCII)(.txt) 2) Portable Document Format (.pdf), ISO 3200 3) Open Office Extended Markup Language (XML) File Formats, ECMA-376, ISO/IEC 29500 i) XML Document Format (.docx) ii) XML Workbook Format (.xlxs) iii) XML Presentation Format (.pptx)	
1.6.2.e	Using a combination of digital signatures and handwritten signatures on a single document, transaction, message, etc. shall be avoided whenever possible, to ensure that a single record can be created where all of the signatures are part of the record and can be validated by Relying Parties.	---
1.6.2.f	In order to facilitate interoperability, DHS implementations of digital signatures shall comply with the PDF Advanced Electronic Signature (PAdES) standard or XML Advanced Electronic Signature (XAdES) standard for digital signature formats.	---
1.6.2.g	For DHS electronic records that are digitally signed, the digital signatures shall be verifiable by relying parties for the entire retention period of the record. The digital signatures shall be verifiable using standard PDVAL protocols (http://www.idmanagement.gov/path-discovery-and-validation).	---
1.6.2.h	When a digital signature is applied to an email by a DHS entity, it shall be for security purposes only, i.e., to enable the recipient or a third party to determine the source of the email and its integrity. Email may be used as a transport mechanism to send documents, transactions, messages, etc., that include legally binding digital signatures, as attachments to an email. If an email is received containing a digital signature that is intended to be legally binding, the source of the email shall be contacted and asked to re-submit the relevant content signed with the legally binding signature as an email attachment, or via another acceptable means.	---
1.6.2.i	A public-private key pair is only valid for the uses specified in the public key's certificate. Only private keys with an associated public key certificate that asserts both the digital signature and non-repudiation bits in the keyUsage	---

Policy ID	DHS Policy Statements	Relevant Controls
	extension shall be used to execute legally binding digital signatures. Digital signatures executed with a private key with associated public key certificate that does not assert both the digital signature and non-repudiation bits in the keyUsage extension shall be rejected (not accepted). Key pairs with associated public key certificates intended for authentication or encryption use shall not be used to execute digital signatures, and digital signatures generated with them shall not be accepted. Authentication certificates, such as the PIV Authentication Certificate and PIV Card Authentication Key certificate, do not assert the non-repudiation key usage bit, and shall not be used to execute digital signatures. Encryption certificates do not assert the digital signature bit or the non-repudiation bit and shall not be used to execute digital signatures. The three certificate types issued by DHS Principal Certificate Authority (CA) (DHS CA4) that are authorized for use for traditional human subscriber digital signatures are: 1) The PIV Digital Signature Certificate, 2) The Non-PIV Human Software Digital Signature Certificate, and 3) The Non-PIV Human Hardware Digital Signature Certificate. The following algorithms are currently authorized for digital signature use: 1) RSA 2048 with SHA-1 and PKCS #1 v1.5 padding 2) RSA 2048 with SHA-256 and PKCS #1 v1.5 padding 3) RSA 2048 with SHA-256 and PSS padding 4) ECDSA P-256 with SHA-256 ecdsa-with-SHA256 5) ECDSA P-384 with SHA-384 ecdsa-with-SHA384 The use of SHA-1 shall be abandoned in favor of SHA-256, as soon as possible.	
1.6.2.j	Digital signatures performed from a mobile device shall only be executed using the Signer's signature key on their PIV or PIV Derived Credential, in accordance with NIST Special Publication 800-157. Implementations of digital signatures to be performed from a mobile device, which are executed using the Signer's signature key from a software-based token and its associated public key certificate issued by DHS Principal CA (DHS CA4), must be authorized by the DHS CISO.	---
1.6.2.k	Public Key Infrastructure (PKI) artifacts (e.g., trust path Certification Authority Certificates, Certificate Revocation Lists (CRL) or Online Certificate Status Protocol (OCSP) Responses) are stapled to a digital signature (i.e., incorporated into the signature data) to ensure that it can be validated in the future. OCSP Responses shall be used instead of CRLs whenever possible, to limit the size of digitally signed electronic records.	---

Policy ID	DHS Policy Statements	Relevant Controls
1.6.2.l	PIN caching shall not be used with legally binding digital signatures. In a session where the user is required to execute multiple legally binding digital signatures, the user shall be required to authenticate himself/herself immediately prior to the execution of each legally binding digital signature.	---
1.6.2.m	The key pairs and associated public key certificates issued to Non Person Entities (NPE) (such as devices, systems, and applications) by the DHS Principal CA (DHS CA4) or acquired from authorized commercial vendors, shall not be used to generate legally binding digital signatures. Certificates issued to NPEs by DHS Internal Use NPE CAs shall only be used for authentication and shall not be used for digital signature.	---

Implementations of digital signatures should adhere, where possible, to the guidance provided in the current versions of the following documents, developed by the DHS Enterprise Digital Signature Capability Integrated Project Team and maintained by the DHS PKI Management Authority:

1) "Using the PIV Card to Digitally Sign Outlook Emails"
2) "Using the PIV Card to Digitally Sign Adobe Acrobat Documents"
3) "Using the PIV Card to Digitally Sign Microsoft Office Documents"

These documents are available for download from the Enterprise Digital Signature folder in the DHS PKI SharePoint site.

1.7 Information Sharing

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

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

The DHS SOC portal implements role-based user profiles that allow Components to use the website's incident database capabilities. Users assigned to Component groups 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 mobile systems such as cell phones and pagers, allow personnel to stay in touch with their offices and wireless local area networks (WLAN) permit connection from various locations throughout a building. While these technologies provide greater flexibility and convenience, they also introduce additional risks.

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

1.8.1 Insider Threats

Managers are generally aware of natural and physical threats, such as earthquakes, tornadoes, fires, floods, electric outages, and plumbing disasters, but may not have the same level of awareness regarding threats originating from within their organizations. The threat from DHS users should not be underestimated. Sensitive information 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 continues to be a threat to DHS systems. Malware and those who employ it have become very sophisticated. Malicious code can be tailored to the recipient. This code can be transferred to an unsuspecting user's machine by various means, including email, visiting infected websites, or across a network. These capabilities may be used to steal, alter, or destroy data; export malicious code to other systems; add backdoors that would permit access to data or network resources; or prevent the legitimate use of the individual computer or network service.

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

1.8.3 Foreign Threats

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

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

Many software manufacturers outsource software code development, which raises concerns about whether or not malicious 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 Director of IT Security Policy and Remediation at infosecpolicy@hq.dhs.gov.

Changes to this policy and to the Handbook may be requested by 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 modification of the *DHS Sensitive Systems Policy Directive 4300A* and *DHS 4300A Sensitive Systems Handbook* (inclusive of all Attachments and appendices).	PL-1
1.9.b	The DHS CISO shall update the *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* at least annually.	PL-1

2.0 ROLES AND RESPONSIBILITIES

Security is 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 (SO) 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 Modernization Act of 2014 (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, networks, and IS-related supply chains. Security 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.
- Establishes and institutionalizes contact with selected groups and associations within the security community:

a. To facilitate ongoing security education and training for organizational personnel;

b. To maintain currency with recommended security practices, techniques, and technologies; and

c. To share current security-related information including threats, vulnerabilities, and incidents.

- Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems: (1) are developed and maintained; and (2) continue to be executed in a timely manner.

- Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
- Implements a threat awareness program that includes a cross-organization information-sharing capability.
- Reviews and approves the tools, techniques, and methodologies planned for use in certifying and authorizing DHS systems, and for reporting and managing systems-level FISMA data. This responsibility includes reviews and approval of Security Control Assessment plans, Contingency Plans, and security risk assessments.
- Consults with the DHS Chief Security Officer (CSO) on matters pertaining to physical security, personnel security, information security, investigations, and Sensitive Compartmented Information (SCI) systems, as they relate to information security and infrastructure.
- Develops and implements procedures for detecting, reporting, and responding to information security incidents.
- Chairs the CISO Council. The Council is composed of all Component CISOs, and is the Department's primary coordination body for any issues associated with information security policy, management, and operations. Component CISOs and 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.
- Provides operational direction to the DHS Security Operations Center (SOC).

2.1.3 Component Chief Information Security Officer

The Component CISO implements and manages all aspects of the Component Information Security Program to ensure compliance with DHS policy and guidance implementing FISMA, other laws, and Executive Orders. The Component CISO 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 PM-6
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, and review and approve ISSO appointments
- Ensure that weekly incident reports are submitted to the DHS 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 adherence to the DHS Secure Baseline Configuration Guides (*DHS 4300A Sensitive Systems 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
- 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 government information and information systems.
- Ensure an acceptable level of trust for each external service, either by accepting risk or by using compensating controls to reduce risk to an acceptable level
- Ensure that systems engineering lifecycle activities implement processes that include software assurance and supply chain risk management
- Issue a Component Supply Chain Risk Management (SCRM) Plan that defines how Component programs and systems shall develop and execute their individual SCRM plans or adopt SCRM into Security Plans

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 shall:

- 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 (*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
- Ensure that ISSOs monitor and manage the information security aspects of supply chain risks
- Ensure that ISSOs adopt software assurance principles and tools

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.

DHS Departmental and Component Risk Executives shall:

- 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, including those associated with the supply chain
- 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

- Ensure that System Owners, ISSOs and AOs monitor and manage supply chain risks, as part of the overall Component risk management strategy.

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

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

Policy ID	DHS Policy Statements	Relevant Controls
2.1.5.a	The DHS CIO shall be the DHS Risk Executive. The DHS CIO has delegated this authority to the DHS CISO.	PL-1, PM-9
2.1.5.b	Each Component CIO shall be the Risk Executive for his or her Component. The Component CIO may delegate this authority to the Component CISO.	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, excluding financial 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, excluding financial 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

Policy ID	DHS Policy Statements	Relevant Controls
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 is assigned in writing to each information system by the Component CISO. 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-2
2.1.7.b	A Security Control Assessor may be responsible for more than one system.	CA-2
2.1.7.c	The Security Control Assessor may take the lead for any or all remedial actions.	CA-7

Policy ID	DHS Policy Statements	Relevant Controls
2.1.7d	The Security Control Assessor provides an assessment of the severity of weaknesses or deficiencies in the information systems, and prepares the final security control 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. Only one ISSO is assigned to a system, but multiple Alternate ISSOs may be designated to assist the ISSO.

While the ISSO performs security functions, responsibility for information system security always rests with the System Owner.

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

Policy ID	DHS Policy Statements	Relevant Controls
2.1.8.a	An ISSO shall be designated for every information system and serve as the point of contact (POC) for all security matters related to that system.	PL-1
2.1.8.b	An ISSO shall ensure the implementation and maintenance of security controls in accordance with the Security Plan (SP) and DHS policies.	PL-1
2.1.8.c	ISSOs shall be federal or contractor employees whose background investigations have been completed in accordance with Section 4 of this Policy.	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. It is strongly encouraged that ISSOs be cleared to the Secret level in order to facilitate intelligence sharing among information security professionals.	---
2.1.8.g	The ISSO shall ensure that timely responses are provided to Infrastructure Change Control Board (ICCB) change request packages.	---

2.1.9 Ongoing Authorization Manager and Operational Risk Management Board

Each Component shall have an Ongoing Authorization (OA) Manager responsible for evaluating and tracking security events for systems operating under the DHS OA Program. Component OA Managers:

- Account for Component risk threshold
- Ensure that Component Risk Executives[see Sec. 2.1.5] are made aware of new risks and security issues
- Facilitate collaboration of the Component IT Security Subject Matter Experts (SME) that serve on the Operational Risk Management Board (ORMB). Component ORMBs determine the criticality of security triggers and the impact of triggers on the security posture of Component systems that are in OA. The ORMB determines the level of each trigger's visibility and recommends to the Component CISO and AO as adjudicators the actions required to mitigate the risks introduced. Refer to the *DHS Ongoing Authorization Methodology* for more information regarding the ORMB.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.9.a	An OA Manager shall be designated for every Component by the Component CISO and serve as the Point of Contact (POC) for all ongoing risk management for all Component systems enrolled in the OA Program.	PL-1
2.1.9.b	OA Manager duties may be assigned as collateral duties for personnel with existing security responsibilities.	PL-1
2.1.9.c	The OA Manager shall have been granted a security clearance and access greater than or equal to the highest level of information contained in Component systems.	---
2.1.9.d	The OA Manager shall ensure that timely analysis (as outlined by the DHS OA Methodology) of identified security events or triggers is provided to the Component ORMB in support of an accountable environment between the ORMB and the OA Manager.	---
2.1.9.e	The Component CISO shall appoint the Chair of the Component ORMB.	---
2.1.9.f	The OA Manager or designee shall be responsible for tracking security events in the monthly Trigger Accountability Log (TRAL), communicating and recording recommendations for Component CISO consumption, and ensuring at least quarterly communication with the AO on system risks.	---

2.1.10 DHS Security Operations Center

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

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

- Review all reported incidents and verify that all pertinent information is recorded, confirmed, and that closure occurs only after all remediation and reporting activities have occurred in accordance with this Policy Directive.
- Focus 24x7 monitoring efforts on shared DHS infrastructure such as the Trusted Internet Connection (TIC), Policy Enforcement Points (PEP), Email Security Gateway (EMSG), Demilitarized Zones (DMZ), Virtual Private Networks (VPN) and other devices as required by DHS CISOs to identify security events of interest that require confirmation, escalation, or declaration as false positive.
- Create Security Event Notifications (SEN) based on monitoring and analysis activities when events of interest are identified that require further investigation.
- Provide oversight on investigational activities and review SENs prior to escalation. SENs will be escalated when Components have sufficiently demonstrated that adequate investigation has been performed and that the event is a verified incident. The Component must provide necessary information regarding the event in accordance with the escalation criteria outlined in Appendix F3, “Response Guidelines”.
- Review all SENs for closure and close SENs after all reasonable investigational activities have been completed.
- Conduct operations and maintenance and approve changes on all security monitoring devices associated with shared DHS infrastructure (such as Intrusion Detection System (IDS), Data Loss Prevention (DLP).
- Provide oversight and guidance for all incidents to ensure adherence to DHS Sensitive Systems Policy Directive 4300A.
- Serve as the primary clearinghouse and collection point for information related to incidents involving DHS systems or networks.
- Coordinate privacy and security incident handling activities with DHS entities such as the DHS Office of Security and the DHS Privacy Office.
- Ensure that remediation and all necessary coordination activities are completed before incident closure.
- Analyze incidents, identifying and notifying other stakeholders and DHS Components and Data Center SOCs that may be affected.

- Provide technical and investigative assistance to Components and Data Center SOCS as needed.
- Provide accurate and timely reports to the DHS CISO on significant incidents and on the status of DHS enterprise computer security.
- Develop and maintain an incident database that contains information on all discovered and reported incidents.
- Provide automated incident notification and reporting to senior DHS and Component leadership and stakeholders such as the DHS Privacy Office and the DHS Office of Security, as well as external reporting entities such as the United States Computer Emergency Readiness Team (US-CERT).
- Update US-CERT on incident status as required.
- Facilitate communications between DHS Components and Data Center SOCS (when applicable) for those incidents involving more than one Component (i.e., Master incidents).
- Provide ad hoc incident trending reports as requested by the DHS CISO.

2.1.11 DHS Component Security Operations Centers

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

- Focus security monitoring efforts on the Component network.
- Compile and maintain a list of mission-critical systems, financial systems, and applications. The list will assist in determining the classification of the Component's systems, and in prioritization of security incidents.
- Component SOCs shall develop and publish internal computer security incident response plans and incident handling procedures, with copies provided to the DHS Enterprise SOC upon request.
- Investigate SENS and Incidents created by the DHS Enterprise SOC and comply with reporting timelines and escalation criteria outlined in *DHS 4300A Sensitive Systems Handbook* Attachment F, "Incident Response," Appendix F3, "Response Guidelines" to either escalate the SEN or close it.
- Monitor internal network enclave traffic such as firewall logs and Network IDS) and host-based security events (e.g. audit logs and Host-based Intrusion Prevention Systems (IPS) and IDS). This includes workstation activity, internal server enclaves, Component-managed externally accessible applications and networks (e.g. DMZ, VPN), and applications hosted by third parties external to DHS.
- Request SEN escalation by the DHS Enterprise SOC, within the reporting timeframes and meeting the escalation criteria outlined in *DHS 4300A Sensitive Systems Handbook* Attachment F, "Incident Response," Appendix F3, "Response Guidelines."
- Conduct SEN and incident investigation including traceback to the host.

- Request closure when a SEN has been identified as inconclusive or as a false positive after providing adequate explanation of investigational activities via the Enterprise Operations Center Portal (EOConline).
- Respond to DHS ENTERPRISE SOC on SEN investigation activities based on the escalation criteria in *DHS 4300A Sensitive Systems Handbook* Attachment F, "Incident Response," Appendix F3, "Response Guidelines."
- Ensure 24x7 incident handling function exists for the Component.
- Lead the Component's incident handling and response activities, including identification, investigation, containment, eradication, and recovery. Coordinate incident response, investigation, and reporting to the DHS Enterprise SOC. Reporting should include all significant data, such as the who, what, when, where, why, and how of a given incident. Coordinate incident handling activities with internal Component entities such as the Component Office of Security, Component Privacy Office, and Internal Affairs.
- Coordinate Component-level remediation efforts as mandated by DHS security policies and communicate remediation activity to DHS Enterprise SOC through EOConline log entries.
- Share applicable information Department-wide or Component-wide, for example by providing network and host-based indicators for malicious logic incidents; such indicators will facilitate implementation of proactive measures to prevent future incidents.
- Provide updates to the DHS Enterprise SOC for significant incidents whenever additional information becomes available.
- Request closure of incidents when Component remediation and mitigation actions have concluded.
- Assist other Components with technical or investigation assistance as requested by the DHS Enterprise SOC.
- Use security automation tools and technologies that facilitate efficient machine and human data exchange with the DHS SOC, with the National Cybersecurity and Communications Integration Center (NCCIC), and with peer SOCs to the maximum extent possible.

2.2 Other Roles

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

2.2.1 Secretary of Homeland Security

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

To that end, the Secretary:

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

2.2.2 Under Secretaries and Heads of DHS Components

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

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, PM-7, PM-8
2.2.3.b	The DHS CIO designates the DHS CISO.	PL-1

The DHS CIO:

- Heads the 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.
- Ensures the development of 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 supply chain risk and risks arising from 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
- Implements firewall changes as requested by DHS and Component CISOs
- 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
- Direct a review of the Component information security program plan be performed with a frequency depending on risk, but no less than annually
- Ensure that an AO has been appointed for every Component information system; serves as the AO for any information system for which no AO has been appointed or where a vacancy exists

- Ensure that information security concerns are addressed by Component Configuration Control Boards, Enterprise Architecture Board (EAB), Acquisition Review Board (ARB), and 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 supply chain risk and 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 the timeframes defined in Attachment F, "Incident Response" of the *DHS 4300A Sensitive Systems Handbook*
- Work with the DHS CIO and Public Affairs Office in preparation for public release of security incident information. The DHS CIO, or designated representative, has sole responsibility for public release of security incident information.
- Ensure compliance with DHS information systems security policy
- Coordinate and advocate resources for information security enterprise solutions

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 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 establishing, overseeing the implementation of, and issuing guidance on DHS privacy policy. The DHS Chief Privacy Officer ensures that the Department's use of technology sustains, and does not erode, privacy protections relating to the collection, use, maintenance, disclosure, deletion, and/or destruction of Personally Identifiable Information (PII). The responsibilities of the DHS Chief Privacy Officer include oversight of all privacy activities within the Department, and ensuring compliance with privacy laws, regulations, and policies.

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

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

Policy ID	DHS Policy Statements	Relevant Controls
2.2.6.a	The DHS Chief Privacy Officer shall review all Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), and System of Records Notices (SORN), providing approval as appropriate.	AR-2, PL-1,

Policy ID	DHS Policy Statements	Relevant Controls
2.2.6.b	The DHS Chief Privacy Officer shall lead and oversee the implementation of and compliance with the NIST SP 800-53 Appendix J, "*Privacy Control Catalog.*" Implementation of Appendix J controls is in coordination with the CIO, CISO, program officials, legal counsel, and others as appropriate. No Authority to Operate (ATO) shall be issued without the DHS Chief Privacy Officer's approval signifying that a system is in compliance with NIST SP 800-53 Appendix J.	AR-1
2.2.6.c	The DHS Chief Privacy Officer shall establish and chairs a Data Integrity Board to review all Computer Matching Agreements (CMA).	DI-2
2.2.6.d	The DHS Chief Privacy Officer shall ensure that the public has access to information about DHS privacy activities and is able to communicate with DHS Privacy Officials; and shall ensure that privacy practices are publicly available through DHS' public facing website.	TR-3
2.2.6.e	The DHS Chief Privacy Officer monitors and audits privacy controls and internal privacy policy during the privacy compliance process to ensure effective implementation.	AR-4
2.2.6.f	The DHS Chief Privacy Officer implements a process for receiving and responding to complaints, concerns, or questions from individuals about DHS' privacy practices.	IP-4

The DHS Chief Privacy Officer, as the SAOP:

- Develops, implements, and maintains a Department-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems
- Monitors federal privacy laws and policy for changes that affect the privacy program
- Allocates sufficient resources to implement and operate the Department-wide privacy program
- Develops a strategic Department privacy plan for implementing applicable privacy controls, policies, and procedures
- Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII
- Updates privacy plans, policies, and procedures biennially

- Oversees privacy incident management, to include providing guidance to Components, and where appropriate coordination with Components responding 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)
- Reviews and approves all Department Privacy Compliance Documentation, including PTAs, PIAs, and SORNs
- Designates Privacy Sensitive Systems as part of the Risk Management Framework based on approved PTAs. Privacy Sensitive Systems are those that maintain PII
- Ensures that the Department meets all reporting requirements mandated by Congress or OMB regarding DHS activities that involve PII or otherwise impact privacy
- Provides department-wide annual and refresher privacy training

2.2.7 DHS Chief Financial Officer

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

Policy ID	DHS Policy Statements	Relevant Controls
2.2.7.a	The DHS CFO, or their designee, shall be the AO for applicable financial systems or mixed financial systems and oversee security control definitions for those systems.	CA-6
2.2.7.b	The DHS CFO has directed that the Component CFO shall be the AO for all applicable 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 comply with the policies defined in Sections 3.5.1 and 3.15.

2.2.8 Program Managers

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

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

Policy ID	DHS Policy Statements	Relevant Controls
2.2.8.a	Program Managers shall ensure that program POA&Ms are prepared and maintained.	CA-5, PM-4
2.2.8.b	Program Managers shall prioritize security weaknesses for mitigation.	CA-5
2.2.8.c	Program Managers shall provide copies of program POA&Ms to affected System Owners.	CA-5, PM-4
2.2.8.d	Program Managers shall ensure that POA&Ms address the following: ▪ known vulnerabilities in the information system ▪ the security categorization of the information system ▪ the specific weaknesses or deficiencies in the information system security controls ▪ the importance of the identified security control weakness or deficiencies ▪ the Component's proposed risk mitigation approach, while addressing the identified weaknesses or deficiencies in the security controls and the rationale for accepting certain weaknesses or deficiencies in the security controls	CA-5 PM-4
2.2.8.e	Program Managers shall determine and document the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need.	AP-1
2.2.8.f	Program Managers shall ensure compliance with SCRM Plans and consider supply chain risks, as identified by the System Owner, when prioritizing security weaknesses for mitigation.	---

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. For proper administration of security, an shall be designated in writing for each system by the AO.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.9.a	System Owners shall ensure that each of their systems is deployed and operated in accordance with this policy document.	PL-1
2.2.9.b	System Owners shall ensure that an ISSO is designated in writing for each information system under their purview.	PL-1
2.2.9.c	There shall be only one System Owner designated for each DHS system.	PL-1
2.2.9.d	The 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
2.2.9.f	The DHS CIO shall designate a System Owner in writing for DHS mission systems and for multi-Component systems.	---
2.2.9.g	The Component CIO shall designate an AO in writing for Component systems.	---
2.2.9.h	Where systems or programs provide common controls, the System Owners shall ensure that a security control assessment is completed in the Information Assurance Compliance System (IACS) for those common controls.	---
2.2.9.i	System Owners shall ensure that risk management activities include addressing supply chain risks for the system's current and all subsequent lifecycle phases and documenting this activity in the SCRM Plan.	---

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.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.10.a	The Common Control Provider shall document all common controls and submit them to the AO.	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 (SAR).	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, 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. (See *DHS 4300A Sensitive Systems Handbook*, Attachment G, "Rules of Behavior."	PL-4

3.0 MANAGEMENT POLICIES

3.1 Basic Requirements

Basic security management principles must be followed in order to ensure the security of 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, wireless mobile device, etc.) shall be individually accounted for as part of a FISMA[1]-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 ensure that every DHS computing resource is identified as an information system or as a part of an information system, either as an Major Application (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
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

[1] *FISMA: Federal Information Security Modernization Act of 2014, Public Law 113-283*

Policy ID	DHS Policy Statements	Relevant Controls
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, for deviations, maintain a waiver approved by the DHS CIO or CISO.	PL-1, PM-1 SA-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, *The Technical Specification for the Security Content Automation Protocol (SCAP)*, including the Common Platform Enumeration (CPE), Common Configuration Enumeration (CCE), and Common Vulnerabilities and Exposures (CVE)	RA-5, SI-2, CM-6

3.2 Capital Planning and Investment Control

Information security is a business driver and any risks found through security testing are ultimately business risks. Information security personnel should be involved, to the maximum extent possible, in all aspects of the acquisition process, including drafting contracts, and procurement documents. DHS Management Directive (MD) 102-01 Rev. 2, *Acquisition Management Directive* and DHS MD 4200.1, *IT Capital Planning and Investment Control (CPIC) and Portfolio Management* provide additional information on these requirements.

Policy ID	DHS Policy Statements	Relevant Controls
3.2.a	System Owners shall include information security requirements in their CPIC business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP) for each DHS system.	PM-3, PM-11, SA-1
3.2.b	System Owners or AOs shall ensure that information security requirements and 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

Policy ID	DHS Policy Statements	Relevant Controls
3.2.c	Component Investment Review Boards (IRB) and Acquisition Review Boards (ARB) shall not approve any capital investment in which the information security requirements, including those that address supply chain threats, 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 Homeland Security Presidential Directive 12 (HSPD-12) implementation.	---

3.3 Contractors and Outsourced Operations

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

Policy ID	DHS Policy Statements	Relevant Controls
3.3.e	Components shall conduct reviews to ensure that information security requirements and provisions to address supply chain risk are included in contract language and that the requirements and provisions 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
3.3.g	Components shall require contractors to apply information system security engineering principles in the specification, design, development, implementation, and modification of information systems, in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-27, *Engineering Principles for Information Technology Security*.	SA-8
3.3.h	For systems with high or moderate impact for any of the Federal Information Processing Standard 199 (FIPS 199) security objectives, Components shall require developers of an information system, system Components, or information system services to: a. Perform Configuration Management (CM) during system, system Component, or service development and implementation b. Document, manage, and control the integrity of changes to items under CM c. Implement only organization-approved changes to the system, system Component, or service d. Document approved changes to the system, system Component, or service and the potential security impacts of such changes e. Track security flaws and flaw resolution within the system, system Component, or service and report findings to the DHS SOC.	SA-10
3.3.i	For systems with high or moderate impact for any of the FIPS 199 security objectives, Components shall require developer of information systems, system Components, or information system services to: a. Create and implement a security assessment plan b. Perform: unit; integration; system; regression testing/evaluation commensurate with the volume and complexity of modifications and the impact to the system risk made by those modifications c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation d. Implement a verifiable flaw remediation process e. Correct flaws identified during security testing/evaluation.	SA-11

Policy ID	DHS Policy Statements	Relevant Controls
3.3.j	All SOW, contract vehicles, and other acquisition-related documents shall include privacy requirements and establish privacy roles, responsibilities, and access requirements for contractors and service providers.	AR-3

3.4 Performance Measures and Metrics

Policy ID	DHS Policy Statements	Relevant Controls
3.4.a	The DHS CISO shall define performance measures to evaluate the effectiveness of the DHS information security program.	---
3.4.b	Components shall provide OMB FISMA data at least monthly to the DHS Compliance Officer.	---
3.4.c	The DHS CISO shall report annually to the Secretary on the effectiveness of the DHS information security program, including the progress of remedial actions.	---
3.4.d	Components shall 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.	AR-6

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)

3.5.1 Continuity of Operations Planning

Policy ID	DHS Policy Statements	Relevant Controls
3.5.1.a	When available, a DHS-wide process for continuity of operations 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 COOPs 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
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 essential 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.	---

3.5.2 Contingency Planning

Policy ID	DHS Policy Statements	Relevant Controls
3.5.2.a	The DHS CIO shall provide guidance, direction, and authority for a standard DHS-wide process for contingency planning for information systems.	CP-1

Policy ID	DHS Policy Statements	Relevant Controls
3.5.2.b	System Owners shall develop and document information system Contingency Plans (CPs) for their information systems, 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 ***availability*** security objective. The minimum contingency capabilities for each impact level are as follows: **High impact** – System functions and information have a high priority for recovery after a short period of loss. **Moderate impact** – System functions and information have a moderate priority for recovery after a moderate period of loss. **Low impact** – System functions and information have a low priority for recovery after prolonged loss.	CP-1
3.5.2.e	CPs shall be developed and maintained by all DHS Components in accordance with the requirements for the FIPS 199 potential impact level for the **availability** security objective. These plans shall be based on three essential phases: Activation/Notification, Recovery, and Reconstitution. Components shall review the CP for the information system at least annually and revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	CP-1, CP-2
3.5.2.f	The DHS CIO shall ensure that CP testing is performed in accordance with the **availability** security objective. The minimum contingency testing for each impact level follows: **High impact** – System recovery roles, responsibilities, procedures, and logistics in the CP shall be tested 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 exercised at least annually to simulate system recovery in a test facility. **Moderate impact** – The CP shall be tested at least annually by reviewing and coordinating with organizational elements responsible for plans within the CP. This may be achieved by performing a walk-through/tabletop exercise. **Low impact** – CP contact information shall be verified at least annually.	CP-4, CP-7

Policy ID	DHS Policy Statements	Relevant Controls
3.5.2.g	The DHS CIO shall ensure that contingency training is performed in accordance with the **availability** security objective. The minimum contingency planning for each impact level follows: **High 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. **Moderate impact** – All system personnel involved in contingency planning efforts shall be trained. Refresher training shall be provided at least annually. **Low impact** – There is no training requirement.	CP-3
3.5.2.h	Components shall coordinate CP testing and/or exercises as appropriate, using COOP-related plans for systems with moderate and high availability FIPS 199 categorization.	CP-4

3.6 Systems Engineering Life Cycle

The DHS Systems Engineering Life Cycle (SELC) is detailed in MD 102-01, "Acquisition Management Directive," Rev.2, Appendix B.

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

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 CM.

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 CM 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.

CM 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

The *DHS 4300A Sensitive Systems Handbook* includes the DHS Secure Baseline Configuration Guides.

Policy ID	DHS Policy Statements	Relevant Controls
3.7.a	Components shall develop and maintain a Configuration Management Plan (CMP) for each information system as part of its system Security Plan (SP). All DHS systems shall be under the oversight of the officer responsible for CM.	CM-1, CM-9
3.7.b	Components shall establish, implement, and enforce CM 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 CM plans and within the timeframe or direction stated in the Information Security Vulnerability Management (ISVM) message published by the DHS Security Operations Center (SOC).	SI-2
3.7.d	System Owners shall document initial system configuration in detail and shall control all subsequent changes in accordance with the CM process.	CM-2, CM-3, CM-9

Policy ID	DHS Policy Statements	Relevant Controls
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 SCAP tool.	---
3.7.g	The System Owner shall request a waiver for information systems that use operating systems or applications that are not hardened or do not follow configuration guidance identified in the DHS Secure Baseline Configuration Guides included in the *DHS 4300A Sensitive Systems Handbook*. Requests shall include a proposed alternative secure configuration.	CM-2, CM-6
3.7.h	Components shall ensure that CM processes under their purview include and consider the results of a security impact analysis when considering proposed changes.	CM-4
3.7.i	Users shall report known or suspected implementations of unauthorized IT changes to DHS Enterprise Configuration Management (ICCB.Services@hq.dhs.gov). For more information regarding how unauthorized changes are addressed, refer to the DHS ICCB Unauthorized Change Tracking Process.	---

3.8 Risk Management

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

Policy ID	DHS Policy Statements	Relevant Controls
3.8.a	Components shall establish a risk management program in accordance with NIST Special Publication (SP) 800-30 Rev 1, "Guide for Conducting Risk Assessments," and with other applicable Federal guidelines.	RA-1

Policy ID	DHS Policy Statements	Relevant Controls
3.8.b	Component CISOs/ISSMs shall ensure that a risk assessment is conducted whenever major modifications that have the potential to significantly impact risk 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-certifications 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 SOCs shall deploy a Component-wide network scanning program.	RA-5
3.8.f	Special rules apply to CFO-designated systems. See Section 3.15 for additional information.	---

3.9 Security Authorization and Security Control Assessments

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

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

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

The DHS *Security Authorization Process Guide* describes detailed processes governing security authorizations.

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

Policy ID	DHS Policy Statements	Relevant Controls
3.9.a	Components shall assign an impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability) for each DHS information system. Components shall apply NIST SP 800-53 and NIST SP 800-161 controls as tailored specifically to the security objective and impact level determined as described in Attachment M to *DHS 4300A, Sensitive Systems Handbook*, "Tailoring the NIST SP 800-53 Security Controls."	PM-10, RA-2
3.9.b	Components shall implement NIST SP 800-53 and NIST SP 800-161 security controls, using the FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems* methodology, based on the FIPS 199 impact level established for each separate security objective (confidentiality, integrity, availability).	---
3.9.c	It is recommended that Components pursue Type Security Authorization for information resources that are under the same direct management control; have the same function or mission objective, operating characteristics, security needs, and that reside in the same general operating environment, or in the case of a distributed system, reside in various locations with similar operating environments. Type Security Authorization shall consist of a master Security Authorization package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites.	---
3.9.d	The AO for a system shall be identified in the Information Assurance Compliance System (IACS). 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 systems 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

Policy ID	DHS Policy Statements	Relevant Controls
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 for a maximum period of 6 (six) months and may grant 1 (one) 6 (six) month extension. Systems under an IATO shall not process sensitive information but may attach to system networks for testing.	PL-1, PM-10
3.9.j	If the system is not fully 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 IACS tools that 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 document the control deficiencies or vulnerabilities, and shall use the plans to correct the deficiencies and vulnerabilities.	CA-5, PM-4
3.9.q	The AO shall formally assume responsibility for operating an information system at an acceptable level of risk. Operating any system 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 waivers.	CA-6, PM-10
3.9.s	Artifacts in support of *new* ATOs shall not be older than 13 months. Older artifacts remain valid during the life of a current ATO.	---
3.9.t	The DHS CIO may revoke the ATO of any DHS information system.	CA-6

Policy ID	DHS Policy Statements	Relevant Controls
3.9.u	The Component CIO may revoke the ATO of any Component-level information system.	CA-6
3.9.v	Components shall assign a common control provider to share controls between systems (e.g., at hosting centers). The authorization package of those common controls must be shared with those operating under 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.	---

3.9.1 Ongoing Authorization

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

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

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

Policy ID	DHS Policy Statements	Relevant Controls
3.9.1.a	Components shall be accepted into the DHS OA Program only with concurrence of the DHS CISO and the Component's AO and/or CIO. All submissions will be considered by DHS CISO using objective eligibility requirements as outlined in the *DHS OA Methodology*.	---
3.9.1.b	Eligible Components may submit requests for systems to join the DHS OA Program. Systems submitted must have a valid ATO at least 60 days from expiration at date of submission (further details are found in the latest version of the *DHS Ongoing Authorization Methodology*).	CA-6, PM-10

Policy ID	DHS Policy Statements	Relevant Controls
3.9.1.c	The DHS CISO shall specify requirements, tools, techniques, and methodologies used to assess and authorize DHS information systems within a Component OA Program.	CA-1, PM-4
3.9.1.d	All DHS systems within the OA Program shall be monitored using the automated Information Assurance Compliance System tools currently in use and approved by the DHS CISO.	CA-1, CA-2, PM-10
3.9.1.e	The DHS OCISO shall maintain a repository for all OA Process documentation and modifications and will communicate changes through the Component CISOs.	CA-1
3.9.1.f	Components shall adhere to established processes and requirements outlined in the *DHS Ongoing Authorization Methodology* to ensure that the OA process is consistent across all DHS Component systems.	CA-1, PM-10
3.9.1.g	The DHS CISO shall review monthly OA deliverables for Component IT systems security compliance for quality and for deficiencies periodically in order to allow continued participation in the DHS OA Program. The DHS CISO may require information systems to revert to previous steps of the NIST Risk Management Framework (RMF), RMF Steps 1-6, in response to OA and/or general information security deficiencies found during periodic quality assurance reviews. Components found unable to sustain OA requirements, or maintain sound security practices (as specified in the Component OA eligibility details of the *DHS OA Methodology*), shall be required to have all or some of their information systems revert to previous steps of the NIST RMF in order to mitigate or compensate for deficiencies found during periodic quality assurance reviews.	CA-6
3.9.1.h	The Component Authorizing Official shall require any of their information systems participating in the DHS OA Program to revert to previous steps of the NIST RMF in order to mitigate or compensate for deficiencies found during periodic quality assurance reviews, in response to system Triggers, changes in supply chain risk, or due to other circumstances which supplies the Component CIO with knowledge of risk to the system or the Component.	CA-6

Policy ID	DHS Policy Statements	Relevant Controls
3.9.1.i	Component CISOs shall designate qualified personnel to fulfill the function of the Operational Risk Management Board (ORMB). The ORMB shall be considered a board of experts representing technical and operational expertise as it relates to Information Security and the Component's information systems, data, and networks. Ideal ORMB roles are detailed in the *DHS OA Methodology*.	---

3.10 Information Security Review and Assistance

Policy ID	DHS Policy Statements	Relevant Controls
3.10.a	Components shall submit their information security policies to the DHS CISO for review.	PL-1
3.10.b	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 information systems security 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 reviews and assistance visits across the Department in order to monitor the effectiveness of Component security programs.	CA-2

3.11 Security Working Groups and Forums

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

3.11.1 CISO Council

The CISO Council and ISSMs constitute the management team responsible for ensuring the development and implementation of 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 for 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 policy.	---

3.11.3 DHS Security Policy Working Group

The OCISO Director responsible for Policy shall chair or appoint the chair for the Security Policy Working Group. The DHS Security Policy Working Group is established to promote collaboration between the Components and Headquarters 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.	---

3.11.4 DHS Enterprise Services Security Working Group

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

Policy ID	DHS Policy Statements	Relevant Controls
3.11.4.a	Each Component CISO shall appoint a representative to the DHS ESSWG.	---
3.11.4.b	Component representatives shall actively participate in the DHS ESSWG.	---

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.

Policy ID	DHS Policy Statements	Relevant Controls
3.12.a	Violations related to information security are addressed in *Standards of Ethical Conduct for Employees of the Executive Branch*; 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

3.13 Required Reporting

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

Policy ID	DHS Policy Statements	Relevant Controls
3.13.a	Components shall collect and submit quarterly and annual information security program status data as required by FISMA.	CA-2 AR-6
3.13.b	Components shall use the automated tool approved by the DHS CISO for the systems authorization process and report generation.	CA-2 AR-6

3.14 Privacy and Data Security

The DHS Privacy Office is responsible for privacy compliance across the Department, including assuring that technologies used by the Department sustain and do not erode privacy protections relating to the use of personal and Departmental information. The DHS Chief Privacy Officer has exclusive jurisdiction over the development of policy relating to Personally Identifiable Information (PII) and to privacy-sensitive programs, systems, or initiatives. Questions from Components 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; 202-343-1717) or refer to the DHS Privacy Office Web page at www.dhs.gov/privacy for additional information.

The privacy controls in NIST SP 800-53 Rev 4, Appendix J are primarily for use by an organization's Senior Agency Official for Privacy (SAOP) and Chief Privacy Officer when working with program managers, mission and business owners, information owners and stewards, Chief Information Officers, Chief Information Security Officers, information system

developers and integrators, and risk executives to incorporate effective privacy protections and practices (i.e., privacy controls) within organizational programs and information systems and the environments in which they operate. The privacy controls facilitate DHS efforts to comply with privacy requirements affecting those department-wide and Component programs and systems that collect, use, maintain, share, or dispose of PII or other activities that raise privacy risks. Unlike the security controls in NIST SP 800-53 Rev 4, Appendix F, which are allocated to the low, moderate, and high baselines given in Appendix D, the privacy controls in Appendix J are selected and implemented based on DHS privacy requirements and the need to protect the PII collected and maintained by DHS information systems and programs, in accordance with Federal privacy legislation, policies, directives, regulations, guidelines, and best practices.

3.14.1 Personally Identifiable Information

Various regulations place restrictions on the Government's collection, use, maintenance, and release of information about individuals. Regulations require agencies to protect PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including 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.*

Consistent with the DHS *Fair Information Practice Principles (FIPPS)*, PII collected and maintained by DHS should be accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices. In addition, DHS adheres to data minimization and retention requirements to collect, use, and retain only PII that is relevant and necessary for the purpose for which it was originally collected. Programs will retain PII for only as long as necessary to fulfill the purpose(s) specified in public notices and in accordance with a record retention schedule approved by National Archives and Records Administration (NARA).

Policy ID	DHS Policy Statements	Relevant Controls
3.14.1.a	When collecting PII, programs shall: a. Confirm to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information; b. Collect PII directly from the individual to the greatest extent practicable; and c. Check for, and correct as necessary, any inaccurate or outdated PII used by its programs or systems through the Privacy Threshold Analysis (PTA) process.	DI-1
3.14.1.b	DHS shall issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.	DI-1
3.14.1.c	Prior to the collection of PII, all programs shall: a. Identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection; and b. Limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent.	DM-1
3.14.1.d	DHS shall conduct an initial evaluation of PII holdings and establish and follow a schedule for regularly reviewing those holdings through the privacy compliance process. The objective of this evaluation is to ensure that only PII that is identified in privacy compliance documentation and other public notices is collected and retained, and that the PII continues to be necessary for accomplishment of a legally authorized purpose.	DM-1
3.14.1.e	Programs and systems that maintain PII shall: a. Retain each collection of PII for the minimum amount of time necessary to fulfill the purpose(s) identified in the notice or as required by law; b. Dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and c. Ensure secure deletion or destruction of PII (including originals, copies, and archived records).	DM-2
3.14.1.f	DHS shall develop policies and procedures that protect and minimize the use of any PII used for testing, training, and research,	DM-3

Additional PII and Sensitive PII-related guidance is 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 Privacy Threshold Analysis (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 Instruction 047-01-001 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 years and a new PTA must be submitted.	AR-2
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.	AR-2
3.14.2.d	Information systems shall not be designated operational until the DHS Privacy Office approves the PTA.	AR-2
3.14.2.e	For Privacy Sensitive Systems, the **confidentiality** security objective shall be assigned an impact level of moderate or higher.	RA-2
3.14.2.f	The PTA process shall be used to maintain a current inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII.	SE-1
3.14.2.g	The PTA process shall be used to ensure that DHS designs information systems to support privacy by automating privacy controls, to the greatest extent feasible.	AR-7

3.14.3 Privacy Impact Assessments

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. 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.	AR-2
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.	AR-2
3.14.3.c	Programs shall use the PIA process to document the means (where feasible and appropriate) for individuals to: 1. Authorize the collection, use, maintaining, and sharing of PII prior to its collection; 2. Understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; 3. Provide consent prior to any new uses or disclosure of previously collected PII; and 4. Consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.	IP-1
3.14.3.d	Programs shall provide effective notice to the public and to individuals regarding: 1. Activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII; 2. Authority for collecting PII; 3. The choices, if any, individuals may have regarding how the program uses PII and the consequences of exercising or not exercising those choices; and 4. The ability to access and have PII amended or corrected if necessary.	TR-1

3.14.3.e	Through effective public notice, programs shall describe: 1. The PII the program collects and the purpose(s) for which it collects that information; 2. How the program uses PII internally; 3. Whether the program shares PII with external entities, the categories of those entities, and the purposes for such sharing; 4. Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; 5. How individuals may obtain access to PII; and 6. How the PII will be protected.	TR-1
3.14.3.f	Programs shall revise all public notices to reflect changes in practice or policy that affect PII or changes in their activities that impact privacy, before or as soon as practicable after any change.	TR-1

PIAs are one tool that DHS uses to convey public notice of information practices and the privacy impact of Department programs and activities. The Department also uses web privacy policies, System of Records Notices (SORN), and Privacy Act Statements to provide effective public notice of program privacy practices. PIAs also document how DHS makes individuals active participants in the decision-making process regarding the collection and use of their PII.

3.14.4 System of Records Notices

The Privacy Act of 1974 requires a SORN when PII is maintained by a Federal agency in a system of records and the PII is retrieved by a personal identifier. A system of records is "*a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual*"[2]. The SORN describes the categories of records and individuals in the system of record; the routine uses of the data; how individuals can gain access to records pertaining to them and correct errors. The term "system of records" is not synonymous with "information system" and can include paper as well as electronic records. SORNs can be written to cover the records in a single group of records or a single information system or they can be written to cover multiple groups of records or multiple information systems.

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

[2] *5 U.S.C. §552a(a)(5) Italics added.*

Records About Individuals" to Circular A-130. DHS has published MD 047-01-001, "Privacy Policy and Compliance," October 6, 2005; and *Official DHS Guidance on System of Records and System of Records Notices.* Information systems that are considered a System of Records must keep an accurate accounting of disclosures of information shared outside of the system.

OMB requires each SORN to be reviewed every two (2) years to ensure that it accurately describes the system of records. This process is called the Biennial SORN Review Process. The DHS Privacy Office works with Components to ensure that SORN reviews are conducted every two 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. SORNs are published in the Federal Register.	TR-2
3.14.4.b	Information systems containing PII shall not be designated operational until a SORN has been published in the Federal Register for 30 days.	CA-6
3.14.4.c	Components shall review and republish SORNs every two years as required by OMB Circular A-130.	TR-2
3.14.4.d	Components shall in their privacy notices, including SORNS, describe the purpose(s) for which PII is collected, used, maintained, and shared.	AP-2
3.14.4.e	Components shall include Privacy Act Statements on all forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.	TR-2
3.14.4.f	Programs shall provide individuals the ability to have access to their PII maintained in its system(s) of records.	IP-2
3.14.4.g	DHS publishes rules and regulations governing how individuals may request access to records maintained in a System of Records.	IP-2
3.14.4.h	Programs shall publish access procedures in SORNs.	IP-2
3.14.4.i	DHS shall adhere to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.	IP-2
3.14.4.j	DHS shall provide a process for individuals to have inaccurate PII maintained by the Department corrected or amended, as appropriate.	IP-3
3.14.4.k	Components shall establish a process for disseminating corrections or amendments of the PII to other authorized users of the PII (such as external information-sharing partners) and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.	IP-3

Policy ID	DHS Policy Statements	Relevant Controls
3.14.4.j	Components shall: 1. Keep an accurate accounting of disclosures of information held in each system of records under its control, including; a. Date, nature, and purpose of each disclosure of a record; and b. Name and address of person or agency to which the disclosure was made; 2. Retain the accounting of disclosures for the life of the record or five years after the disclosure, whichever is longer; and 3. Make the accounting of disclosures available to the person named in the record upon request.	AR-8

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

- *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security*
- *DHS 4300A Sensitive System Handbook,* Attachment S: "Compliance Framework for Privacy Sensitive Systems"
- *DHS 4300A Sensitive Systems Handbook,* Attachment S1: "Managing Computer-Readable Extracts Containing Sensitive PII."

In addition, see Section 5.3 of this Policy Directive 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, equipment or mobile devices 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

Policy ID	DHS Policy Statements	Relevant Controls
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 SP) 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 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 90 days unless the information included in the extracts is required beyond that period. Permanent erasure of the extracts or the need for continued use of the data shall be documented by the Data Owner and audited periodically by the Component Privacy Officer or Privacy Point of Contact (PPOC).	---

3.14.6 Privacy Incident Reporting

The DHS Privacy Office is responsible for implementing the Department's privacy incident response program based on requirements outlined in OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007. 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 immediately coordinate with the Component Privacy Officer or PPOC and Component CISO/ISSM to evaluate and subsequently report the incident to the DHS SOC 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

Policy ID	DHS Policy Statements	Relevant Controls
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 *all* types of privacy incidents, whether or not they involve information resources. This unitary reporting process shall remain in effect until each Component has a Privacy Officer or PPOC who can fulfill the reporting duties.	IR-6
3.14.6.d	DHS personnel shall also report suspected or confirmed privacy incidents 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.	---

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-04-04, *E-Authentication Guidance for Federal Agencies*
- NIST SP 800-63, *Electronic Authentication Guideline*

Policy ID	DHS Policy Statements	Relevant Controls
3.14.7.a	For systems that allow online transactions, Components shall determine whether e-authentication requirements apply.	IA-2
3.14.7.b	Components shall determine the appropriate assurance level for e-authentication by following the steps described in OMB M-04-04, *E-Authentication Guidance for Federal Agencies*.	IA-2
3.14.7.c	Components shall implement the technical requirements described in NIST SP 800-63, *Electronic Authentication Guideline*, at the appropriate assurance level for those systems with e-authentication requirements.	IA-2

Policy ID	DHS Policy Statements	Relevant Controls
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.	AR-2
3.14.7.f	Existing physical and logical access control systems shall be upgraded to use Personal Identification Verification (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.	---
3.14.7.i	For systems with high or moderate impact for any of the FIPS 199 security objectives information systems shall uniquely identify and authenticate network devices before establishing a network connection.	IA-3

3.14.8 Use Limitation and External Information Sharing

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

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

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

Policy ID	DHS Policy Statements	Relevant Controls
3.14.8.a	Programs use PII *within DHS* only for the authorized purpose(s) identified in the Privacy Act or in public notices such as PIAs and SORNs.	UL-1
3.14.8.b	Programs share PII *outside of DHS* only for the authorized purposes identified in the Privacy Act or described in PUBLIC notice(s) such as PIAs and SORNs or for a purpose that is compatible with those purposes.	UL-2
3.14.8.c	Components, where appropriate, enter into Memorandums of Understanding, Memorandums of Agreement, Letters of Intent, CCMAs, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used.	UL-2
3.14.8.d	Component Privacy Officers monitor, audit, and train their staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.	UL-2
3.14.8.e	Component Privacy Officers evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether new or updated public notice is required.	UL-2
3.14.8.f	All Computer Matching Agreements shall be reviewed by the Data Integrity Board, chaired by the DHS Chief Privacy Officer.	DI-2

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*. Controls required to be assessed annually for CFO Designated Systems may be found documented in Attachment R, "Compliance Framework for CFO Designated Financial Systems" to the *DHS 4300A Sensitive Systems Handbook*. Attachment R is limited to the controls that must be reviewed annually (and does not contain the requirements of OMB Circular 123).

These requirements are in addition to both the other security requirements established in this Policy Directive and to other system Line of Business requirements developed by the CFO.

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 IACS. This includes updating the security control assessment and 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 the CFO Designated System 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**s 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 *all* CFO Designated Systems requiring moderate availability and that Disaster Recovery Plans are created for *all* CFO-designated systems requiring high availability and that each plan is tested annually, and results with lessons learned annually.	CP-2, CP-4
3.15.g	Component CISOs/ISSMs shall ensure that weekly incident response tracking is performed for all of their respective CFO-designated systems.	IR-5
3.15.h	Component CISOs/ISSMs shall ensure that incidents related to their respective CFO-designated systems are reported to the Component CFO.	IR-4, IR-6
3.15.i	The SP shall be updated for CFO-designated systems at least annually. Key controls prescribed in Attachment R, *Compliance Framework for CFO-designated systems* shall be identified in the SP.	PL-2
3.15.j	Component CISOs/ISSMs must request a waiver from the DHS CISO if a key control weakness is identified for a CFO-designated System and not remediated within 12 months.	CA-5, CA-7

Policy ID	DHS Policy Statements	Relevant Controls
3.15.k	Component CFOs shall ensure that a full time dedicated ISSO is assigned to each CFO-designated System. CFO-designated System ISSOs may be assigned to more than one CFO Designated System.	---
3.15.l	CFO Designated System ATOs shall be rescinded if Components fail to comply with testing and reporting requirements established within this policy.	CA-1, CA-6
3.15.m	Component CFOs shall work with their Component CISOs/ISSMs to approve any major system changes to CFO-designated systems identified in the DHS inventory.	CA-1, CM-8

3.16 Social Media

Due to the high threat of malware, Social Media host sites have been blocked at the Trusted Internet Connection (TIC). 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).

Policy ID	DHS Policy Statements	Relevant Controls
3.16.a	Only OPA-designated Content Managers (Department level and Component level) may post content on behalf of DHS or representing DHS, and only those individuals designated by OPA for this purpose shall be granted access on a continuing basis.	CM-10
3.16.b	Posted content shall be in alignment 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).	---
3.16.c	Under no circumstances shall sensitive information be posted to social media sites.	--
3.16.d	Content shall not be posted to any social media site for which the Department has not approved and published *both* final posting guidelines *and* TOS.	CM-10
3.16.e	Content Managers shall review and understand the appropriate Department-level TOS for the appropriate social media host.	---

Policy ID	DHS Policy Statements	Relevant Controls
3.16.f	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.	---

3.17 Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[3] addresses the privacy of individuals' health information by establishing a Federal privacy standard for health information and how it can be used and disclosed.

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

Because of the diverse mission of DHS, it may be necessary for some Components to collect PHI as part of a larger mission requirement (for example detainee processing, disaster relief, etc.). This section applies to all Components and personnel who collect, process, or store PHI (refer to NIST SP 800-66 Rev 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, 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 and privacy 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] *Public Law 104-191*

Policy ID	DHS Policy Statements	Relevant Controls
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 technologies allow DHS to address demands for better information services; conserve resources; consolidate systems; and improve security. The essential characteristics of cloud computing (on-demand provisioning, resource pooling, elasticity, network access, and measured services) provide the potential for DHS to reduce procurement and operating costs and increase service efficiency.

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

The purposes of FedRAMP are:

- To improve the consistency and quality of information security in the cloud
- To ensure trustworthy and re-usable documentation and assessment of security controls
- To provide ongoing assurance and risk assessment of select cloud services. Cloud services are discussed on the FedRAMP Web site at http://www.gsa.gov/portal/category/102371 .
- To enable rapid and cost-effective procurement of information systems and services for Federal agencies.

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

- Federal agency customers
- Cloud Service Providers (CSP)
- Joint Authorization Board (JAB)
- Third Party Assessors (3PAO)
- FedRAMP Program Management Office (PMO)
- National Institute of Standards and Technology (NIST)

NIST SP 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." All uses of cloud computing by DHS will follow DHS security authorization processes and procedures to include a completed security authorization package and an ATO signed by the appropriate Authorizing Official. Those cloud systems and services which are not exempt from FedRAMP requirements will use the FedRAMP

process as required by OMB. Organizations should also review Section 3.14 for applicability in cloud environments if they are dealing with privacy data.

Policy ID	DHS Policy Statements	Relevant Controls
3.18.a	Components shall leverage cloud services with FedRAMP Provisional Authority to Operate (P-ATO) whenever available when authorizing cloud systems or services. When a P-ATO is not available, Components shall leverage FedRAMP compliant Agency ATO packages whenever available to the fullest extent possible.	---
3.18.b	All DHS cloud services of FIPS Moderate categorization or higher, consumed by or intended to be consumed by multiple government organizations outside of DHS, shall submit to FedRAMP for JAB Provisional Authorization.	---
3.18.c	The use of cloud systems and services shall follow existing DHS security authorization processes and procedures to include a completed security authorization package and an ATO signed by the Component or DHS-designated Authorizing Official.	---
3.18.d	All DHS cloud systems and services not exempt from FedRAMP shall use appropriate FedRAMP documentation templates, be assessed using the JAB-approved security-control baselines and additional DHS requirements, and be categorized in the FISMA inventory as either a General Support System or a Major Application. DHS cloud systems and services shall not be categorized as External Information Systems (EIS).	---
3.18.e	All DHS cloud systems and services not exempt from FedRAMP shall use the FedRAMP process and security authorization requirements when initiating, reviewing, granting and revoking risk assessments and security authorizations.	---

4.0 OPERATIONAL POLICIES

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 Citizenship, Personnel Screening, and Position Categorization

Policy ID	DHS Policy Statements	Relevant Controls
4.1.1.a	Components shall designate the position sensitivity level for all Government and contractor positions that use, develop, operate, or maintain information systems and shall determine risk levels for each contractor position. Position sensitivity levels shall be reviewed annually and revised as appropriate.	PS-2, PS-3, PS-7
4.1.1.b	Components shall ensure 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 any Federal employee granted access to any DHS system has a favorably adjudicated Tier 2 Investigation (formerly Moderate Risk Background Investigation [MBI]) as defined in DHS Instruction 121-01-007, *Personnel Suitability and Security Program*, 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 Justice (UCMJ) shall be exempt from this requirement.	PS-3
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 Department of Homeland Security Acquisition Regulation (HSAR) and the DHS Instruction 121-01-007, *Personnel Suitability and Security Program*, 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 requested by submitting a completed Foreign National Visitor Access Request form for each foreign national to the DHS Office of the Chief Security Officer (OCSO), in accordance with Section 1.5.2, of this policy, "Requests for Exception to U.S. Citizenship Requirement."	PS-3
4.1.1.f	Components shall ensure that no temporary employee is granted access to any DHS system without having met the review and investigation standard defined in DHS Instruction 121-01-007, "Personnel Suitability and Security Program," Chapter 2: "Federal Employee/Applicant Suitability Requirements."	--

4.1.2 Rules of Behavior

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

4.1.3 Access to Sensitive Information

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

4.1.4 Segregation of Duties and Least Privilege

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

Policy ID	DHS Policy Statements	Relevant Controls
4.1.4.a	Components shall divide and separate duties and responsibilities of critical information system functions among different individuals to minimize the possibility of any one individual having 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 Authorizing Official (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

Policy ID	DHS Policy Statements	Relevant Controls
4.1.4.d	Administrator accounts shall be used only for performing required administrator duties. Individuals shall use their regular user accounts to perform all other functions not directly tied to administrator duties (checking email, accessing the Internet).	AC-6

4.1.5 Information Security and Privacy Awareness, Training, and Education

Policy ID	DHS Policy Statements	Relevant Controls
4.1.5.a	Components shall establish an information security training program for users of DHS information systems.	AT-1
4.1.5.b	DHS personnel, contractors, or others working on behalf of DHS (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 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-4
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's 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

Policy ID	DHS Policy Statements	Relevant Controls
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 at the request of the DHS Information Security Training Program Office provide evidence of training by submitting copies of training schedules, training rosters, and training reports.	AT-4
4.1.5.j	The DHS CISO shall review Component information security awareness and role-based training programs annually.	AT-1
4.1.5.k	Components shall submit a roster 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-3
4.1.5.l	The annual security awareness training shall include incident response training to information system users consistent with assigned roles and responsibilities. (Initial training shall be completed within twenty-four (24) hours of assuming an incident response role or responsibility. Out of cycle refresher training shall be conducted as required due to information system changes)	IR-2
4.1.5.m	Components shall develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.	AR-5
4.1.5.n	Components shall administer basic privacy training annually and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII annually.	AR-5
4.1.5.o	Components shall ensure that personnel annually certify (manually or electronically) acceptance of responsibilities for privacy requirements.	AR-5

4.1.6 Separation from Duty

Policy ID	DHS Policy Statements	Relevant Controls
4.1.6.a	Components shall implement procedures to ensure that system 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, PS-5
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
4.1.6.e	Components shall develop and document access agreements for information systems and ensure that individuals requiring access to information and information systems sign appropriate access agreements prior to being granted access, and re-sign whenever access agreements have been updated. Access agreements shall be reviewed at least annually,	PS-6

4.2 Physical Security

4.2.1 General Physical Access

Policy ID	DHS Policy Statements	Relevant Controls
4.2.1.a	Access to DHS buildings, rooms, work areas, spaces, and structures housing information systems, equipment, and data shall be limited to authorized personnel.	PE-2
4.2.1.b	Controls for deterring, detecting, restricting, and regulating access to sensitive areas shall be in place and shall be sufficient to safeguard against possible loss, theft, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters.	PE-3
4.2.1.c	Controls shall be based on the level of classification and risk, determined in accordance with Departmental security policy as reflected in this and other relevant documents.	PE-1, PM-9

Policy ID	DHS Policy Statements	Relevant Controls
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-2, PE-3, PE-6, PE-8
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.	---
4.2.1.f	Components shall control physical access to transmission medium that transmits unencrypted data within Component facilities using DHS SOC-approved safeguards.	PE-4
4.2.1.g	Components shall control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	PE-5
4.2.1.h	Components shall: a. Protect power equipment and power cabling for the information systems from damage and destruction b. Provide capability to shut off power to the information system or individual system Components in emergency situations c. Place emergency shutoff switches or devices to facilitate safe and easy access for personnel d. Protect emergency power shutoff capability from unauthorized activation e. Provide a short-term uninterruptible power supply to facilitate either an orderly shutdown of the information system or a transition of the information system to long-term alternate power in the event of a primary power source loss.	PE-9, PE-10, PE-11

Policy ID	DHS Policy Statements	Relevant Controls
4.2.1.i	Components shall: a. Employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility b. Employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source c. Maintain and monitor temperature and humidity levels within the facility where information systems reside d. Protect information systems from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	PE-12, PE-13, PE-14, PE-15
4.2.1.j	Components shall authorize, monitor, control and maintain records of the delivery and removal of hardware and software that enters and exits a facility.	PE-16
4.2.1.k	Components shall: a. Employ security at an alternate work site that is commensurate with the security categorization level of the information processed and that supports an organizational risk assessment b. Assess as feasible, the effectiveness of security controls at alternate work sites c. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.	PE-17

4.2.2 Sensitive Facility

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

4.3 Media Controls

4.3.1 Media Protection

Policy ID	DHS Policy Statements	Relevant Controls
4.3.1.a	Components shall ensure that all media containing sensitive information, including hard copy media, backup media, and removable media such as Universal Serial Bus (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 (such as USB drives) and from connecting them to DHS equipment or networks or using them to store DHS sensitive information.	MP-2
4.3.1.d	All USB drives shall use encryption in compliance with Section 5.5.1 of this Policy Directive.	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 Management Directive (MD) 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, for the transportation or mailing of sensitive media.	MP-5

4.3.2 Media Marking and Transport

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

4.3.3 Media Sanitization and Disposal

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

4.3.4 Production, Input/Output Controls

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

4.4 Voice Communications Security

4.4.1 Private Branch Exchange

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

4.4.2 Telephone Communications

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

4.4.3 Voice Mail

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

4.5 Data Communications

4.5.1 Telecommunications Protection Techniques

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

Policy ID	DHS Policy Statements	Relevant Controls
	cost-effective alternatives to the use of encryption for sensitive information requiring telecommunications protection.	
4.5.1.b	In cases with high impact and moderate impact for any of the FIPS 199 security objectives, Components shall establish alternate telecommunications services including necessary agreements to permit the resumption of specified operations for essential missions and business functions within a Component-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	CP-8

4.5.2 Facsimiles

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

4.5.3 Video Teleconferencing

Policy ID	DHS Policy Statements	Relevant Controls
4.5.3.a	Components shall implement controls to ensure that only authorized individuals are able to participate in each 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
4.5.3.c	Video teleconferencing equipment and software shall be disabled when not in use.	AC-3, PE-3

4.5.4 Voice over Data Networks

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

Policy ID	DHS Policy Statements	Relevant Controls
4.5.4.a	Prior to implementing voice over data network technology, Components shall conduct rigorous risk assessments and security testing and provide a business justification for its 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

4.6 Wireless Network Communications

Wireless network communications technologies include the following:

- Wireless systems (e.g., Wireless Local Area Networks [WLAN], Wireless Wide Area Networks [WWAN], Wireless Personal Area Networks [WPAN], peer-to-peer wireless networks, information systems that leverage commercial wireless services). Wireless systems include the transmission medium, stationary integrated devices, firmware, supporting services, and protocols
- Wireless mobile devices capable of storing, processing, or transmitting sensitive information (e.g., Personal Digital Assistants [PDA], smart telephones, two-way pagers, handheld radios, cellular telephones, Personal Communications Services [PCS] devices, multifunctional wireless devices, portable audio/video recording devices with wireless capability, scanning devices, messaging devices)
- Wireless tactical systems, including mission-critical communication systems and devices (e.g., include Land Mobile Radio [LMR] subscriber devices and infrastructure equipment, remote sensors, technical investigative communications systems)

- Radio Frequency Identification (RFID)

Policy ID	DHS Policy Statements	Relevant Controls
4.6.a	Components shall not introduce new wireless network communications technologies into the enterprise unless the appropriate AO specifically approves a technology and application.	AC-18
4.6.b	Components using Public Key Infrastructure (PKI)-based encryption on any wireless device shall implement and maintain a key management plan approved by the DHS PKI Policy Authority.	IA-5, SC-12

4.6.1 Wireless Systems

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

Policy ID	DHS Policy Statements	Relevant Controls
4.6.1.a	Annual information security assessments shall be conducted on all approved wireless systems. Wireless information security assessments shall enumerate vulnerabilities, risk statements, risk levels, and corrective actions.	CA-2, PM-9
4.6.1.b	Plans 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 any non-GFE wireless device.	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 waiver to policy from the DHS CISO.	CA-5

Policy ID	DHS Policy Statements	Relevant Controls
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 (1) establish usage restrictions and implementation guidance for wireless technologies; and (2) authorize, monitor, and control wireless access to DHS information systems.	AC-18

4.6.2 Wireless Mobile Devices

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

Biometrics may be harvested and are not a secret (in cryptographic terms). For this reason, biometrics should not be utililzed as a single-factor authentication mechanism for *sensitive information*. Component AO's and CISO's should carefully assess the residual risks when authorizing biometric use in mobile device operations.

Guidance applicable to wireless mobile devices is detailed in *DHS 4300A Sensitive Systems Handbook* Attachment Q2, "Mobile Devices."

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.a	Components shall ensure that neither personally-owned wireless mobile devices nor Government-owned wireless mobile devices are permitted in conference rooms or secure facilities where classified information is discussed. Wireless mobile devices and accessories are prohibited in areas where unclassified, sensitive information is discussed, maintained, or distributed unless specifically authorized in writing by the AO(s) for the system(s) used in the area.	AC-19, PL-4; PE-18
4.6.2.b	Wireless mobile devices 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

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.c	Wireless mobile devices that store, process, or transmit sensitive information shall implement full-disk encryption using NIST FIPS 140-2 Validated encryption modules[4] and strong complex passwords prior to receiving sensitive information. A strong complex password shall be required to decrypt after any power cycling or restart.	AC-19, IA-5, IA-7
4.6.2.d	The AO shall approve the use of wireless mobile devices or software applications used to process, store, or transmit sensitive information from the NSA Commercial Solutions for Classified (CSFC) Program components list[5]; FIPS 201 Approved Products List (APL)[6]; or the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) product list[7]. Mobile devices approved by the AO must be posted in the DHS Enterprise Architecture (EA) Approved Products List (APL) of the Technical Reference Model (TRM).	AC-19, CA-6, IA-7, SC-8, SC-9, SC-13
4.6.2.e	Device mobile code will be downloaded and installed only as approved by the AO. Mobile code approved by the AO must be posted in the DHS Enterprise Architecture (EA) Approved Products List (APL) of the Technical Reference Model (TRM).	SC-18
4.6.2.f	Wireless mobile device operation is permitted only when Component CISO - approved anti-malware software and software patches are current. Anti-malware and software patch versions approved by the Component CISO must be posted in the DHS Enterprise Architecture (EA) Approved Products List (APL) of the Technical Reference Model (TRM).	SI-3
4.6.2.g	The AO will approve appropriate cost-effective countermeasures against denial-of-service attacks prior to wireless device operation.	SC-5 SC-7
4.6.2.h	Components shall maintain a current inventory of all approved wireless mobile devices in operation. The inventory must be posted in the DHS inventory management system.	PM-5

[4] *A list of FIPS 140-2 validated encryption is located at* http://csrc.nist.gov/groups/STM/cmvp/validation.html

[5] *A list of NSA CSFC Program components is located at* https://www.nsa.gov/ia/programs/csfc_program/component_list.shtml.

[6] *The FIPS-201 Approved Products List is located at* http://www.idmanagement.gov/approved-products-list

[7] *A list of NIAP-CCEVS products is located at* https://www.niap-ccevs.org/CCEVS_Products

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.i	Wireless mobile devices shall be sanitized of all information before being reused by another individual, office, or Component within DHS or before they are retired. Wireless mobile devices that are disposed of, recycled, or returned to the owner or manufacturer shall first be sanitized using procedures approved by the AO using NSA-approved media destruction methods as appropriate[8].	MP-6
4.6.2.j	Wireless mobile devices not compliant with DHS information security policy require a migration plan outlining the provisions, procedures, and plans for transitioning these wireless mobile devices to meet 4300A requirements. Operation of these non-compliant systems requires an approved waiver from the DHS CISO.	CA-5 CA-6
4.6.2.k	AOs may authorize use of Biometric tokens as an authentication factor when the mobile device implements physical isolation of secure memory for storage of biometric data and trusted execution environment for reading and processing biometrics	
4.6.2.l	If authorized for use, fingerprint sensors must be touch-based (vs. swipe-based) and must read and process data in a trusted execution environment separated from access by other processes	
4.6.2.m	The use of add-on devices, such as cameras and video/voice recorders, is not authorized unless approved by the AO. Functions that can record or transmit sensitive information via audio, video, Infrared (IR), or Radio Frequency (RF) shall be disabled or powered off in areas where sensitive information is discussed.	AC-19, CM-7, PE-18, SC-7
4.6.2.n	When Biometric fingerprint technology is used as a subsequent unlock method on a mobile device; it shall be configured to allow no more than five (5) consecutive failed fingerprint attempts and upon failure of these attempts require entering the complex password.	AC-19, IA-7, SC-8, SC-9, SC-13
4.6.2.o	Mobile devices shall be configured to lock after a maximum of 10 minutes idle.	
4.6.2.p	Mobile devices shall be configured to lock after a maximum of 10 sequential unsuccessful attempts to gain access.	

[8] *The NSA Media Destruction guidance is located at*
https://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.q	Components shall ensure that use of a device's native biometric fingerprint authentication technology is permitted by and in compliance with the published DHS Configuration Guide for the device.	
4.6.2.r	When derived PIV credentials are utilized and stored in a FIPS 140-2 validated (a) native device hardware keystore or (b) Mobile Device Manager's (MDMs) software-based keystore; the credential shall be activated by either a knowledge-based or biometric token.	

4.6.2.1 Cellular Phones

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

4.6.2.2 Pagers

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

4.6.2.3 Multifunctional Wireless Devices

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

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

4.6.2.4 Bluetooth

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.4.a	Bluetooth functionality shall be disabled when not in use.	AC-18 CM-6 SC-8 SC-13
4.6.2.4.b	Master devices (those that have unidirectional control over one or more other devices, such as a smartphone and headset combination) shall include link activity status indicators such as icons or LEDs.	AC-18 CM-6 SC-8 SC-13

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.4.c	Pairing shall be performed as infrequently as possible.	AC-18 CM-6 SC-8 SC-13
4.6.2.4.d	Devices shall use low power to minimize the range of communication.	AC-4 PE-3 PE-18 PE-19
4.6.2.4.e	Devices shall be configured for manual pairing and shall prompt the user to authorize any incoming connection requests; auto pairing shall not be used.	AC-18 CM-6 SC-8 SC-13
4.6.2.4.f	Devices shall be maintained in non-discoverable mode except during device pairing.	AC-18 CM-6 SC-8 SC-13
4.6.2.4.g	Multiple or split communication paths shall not be used on devices.	AC-3 AC-18
4.6.2.4.h	Pairings shall only be made between approved devices. Devices may be paired to receivers in personally owned vehicles for voice communication as approved by the AO.	AC-18 AC-19 AC-20
4.6.2.4.i	Profiles shall be deleted for devices no longer in service.	AC-18 CM-6 SC-8 SC-13
4.6.2.4.j	Devices shall be transported and stored securely at all times.	---

For additional information, please refer to "Bluetooth Security," Attachment Q 6 to *DHS 4300A Sensitive Systems Handbook*.

4.6.3 Wireless Tactical Systems

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

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

Policy ID	DHS Policy Statements	Relevant Controls
4.6.3.a	AOs shall be immediately notified whenever any security feature is 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
4.6.3.c	Cost-effective countermeasures to denial-of-service attacks shall be identified and implemented prior to a wireless tactical system being approved for use.	SC-5
4.6.3.d	Components shall maintain a current inventory of all approved wireless tactical systems in operation.	PM-5
4.6.3.e	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 from the DHS CISO, as appropriate.	---
4.6.3.f	The security configuration of LMR subscriber units shall be validated via over-the-air-rekeying (OTAR) or hard rekey using a crypto-period no longer than 180 days.	SC-12
4.6.3.g	All LMR systems shall comply with Project 25 (P25, EIA/TIA-102) security standards where applicable.	CM-2

4.6.4 Radio Frequency Identification

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

RFID procedures are described in "Sensitive RFID Systems," Attachment Q4 to *DHS 4300A Sensitive Systems Handbook.*

Policy ID	DHS Policy Statements	Relevant Controls
4.6.4.a	Components implementing RFID systems shall assess hazards of	PE-18

Policy ID	DHS Policy Statements	Relevant Controls
	electromagnetic radiation to fuel, ordnance, and personnel before deployment of the RFID technology.	
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.	AR-2, AC-6
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

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

4.8 Equipment

4.8.1 Workstations

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

4.8.2 Laptop Computers and Other Mobile Computing Devices

Policy ID	DHS Policy Statements	Relevant Controls
4.8.2.a	Information stored on any laptop computer or other mobile computing device that may be used in a residence or on travel shall use encryption in accordance with Section 5.5.1, Encryption, for data at rest and in motion. Passwords, tokens and Smart Cards shall not be stored on or with the laptop or other mobile computing device.	AC-19, IA-2, SC-12, SC-28
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 using one of the following methods: • a locked office • a locking cable • a locked cabinet • a locked desk	AC-19, PE-3, PL-4
4.8.2.d	Users shall obtain the written approval of the office director before taking a laptop computer or other mobile computing device outside of the United States or its territories.	AC-19, PL-4

4.8.3 Personally Owned Equipment and Software

Policy ID	DHS Policy Statements	Relevant Controls
4.8.3.a	Personally owned equipment and software shall not be used to process, access, or store sensitive information without the written prior approval of the AO.	CM-10, CM-11

Policy ID	DHS Policy Statements	Relevant Controls
4.8.3.b	Equipment that is not owned or leased by the Federal Government, or operated by a contractor on behalf of the Federal Government, shall not be connected to DHS equipment or networks without the written prior approval of the Component CISO/ISSM.	SA-9
4.8.3.c	Any device that has been obtained through civil or criminal asset forfeiture shall not be used as part of a DHS information system nor used to process DHS data.	AC-20

4.8.4 Hardware and Software

Policy ID	DHS Policy Statements	Relevant Controls
4.8.4.a	Components shall ensure that DHS information systems follow the hardening guides for operating systems and the configuration guides for applications published by the DHS CISO. *DHS 4300A Sensitive Systems Handbook* 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 CM 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. When the technology is available, Components shall ensure that their systems are protected against pass-the-hash and lateral movement vulnerabilities.	CM-3, RA-5
4.8.4.e	Components shall ensure that maintenance ports are disabled during normal system operation and enabled only during approved maintenance activities.	MA-1
4.8.4.f	System libraries shall be managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.	SI-7
4.8.4.g	Components shall develop maintenance policy and procedures.	MA-1
4.8.4.h	If cleared maintenance personnel are not available, a trusted DHS employee with sufficient technical knowledge to detect and prevent unauthorized modification to the information system or its network shall monitor and escort the maintenance personnel during maintenance activities. This situation shall only occur in exceptional cases. Components shall take all possible steps to ensure that trusted maintenance personnel are available.	MA-5
4.8.4.i	Maintenance using a different user's identity may be performed only when the user is present. The *user* shall log in and observe the maintenance actions at all times. *Users shall not share their authentication information with maintenance personnel.*	MA-5

Policy ID	DHS Policy Statements	Relevant Controls
4.8.4.j	Components shall define and utilize a process for the scheduling, performance, approvals, documenting, testing, and clearing of equipment requiring maintenance. The process shall protect sensitive information by requiring authorized personnel to explicitly: a. Approve the removal of an information system or system Components from organizational facilities for off-site maintenance or repairs; b. Sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and c. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.	MA-2
4.8.4.k	Components shall approve, control, and monitor information system maintenance tools.	MA-3
4.8.4.l	Components shall obtain information system maintenance support and/or spare parts within a Component-defined time period after failure.	MA-6
4.8.4.m	Components shall include requirements for software assurance and supply chain risk management prior to acquisition of any hardware or software products. Components shall ensure that commercial-off-the-shelf (COTS) hardware and software products in use by or being considered for use in moderate and high criticality systems, shall be analyzed for supply chain risk prior to acquisition activities that procure new products, upgrade existing products, or that will integrate these products with commercial services.	

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

Policy ID	DHS Policy Statements	Relevant Controls
4.8.5.a	DHS employees may use Government office equipment and DHS systems/computers for authorized purposes only. "Authorized use" includes limited personal use as described in DHS MD 4600.1, *Personal Use of Government Office Equipment*, and DHS MD 4900, *Individual Use and Operation of DHS Information Systems/Computers*.	---

Policy ID	DHS Policy Statements	Relevant Controls
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.	---

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 information.	CM-7
4.8.6.b	In cases where valid mission requirements or equipment limitations prevent disabling wireless capabilities, Components shall comply with all requirements outlined in Section 4.6, Wireless Communication *and* obtain a waiver in accordance with this policy.	CM-7, IR-4, IR-6

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.

The CIO is responsible for implementing firewall changes in a timely manner.

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 shall be operationally subordinate to the DHS SOC, which shall provide them operational oversight and guidance. HSDN SOC will oversee the handling of all incidents occurring on HSDN and coordinate the sharing of incident information with DHS SOC.	IR-1, IR-4, IR-6

Policy ID	DHS Policy Statements	Relevant Controls
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. DHS SOC is responsible for monitoring shared infrastructure such as the Trusted Internet Connection (TIC), Policy Enforcement Points (PEP), and Email Secure Gateway (EMSG). Component SOCs are responsible for monitoring at a minimum internal enclave network traffic and internal host network and host-based activity.	---
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 the DHS C-LAN. 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 Digital Malware Analysis (DMA) 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. Components are required to comply with the ISVMs released by the DHS SOC. 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 pertinent matters involving the security of information systems and that security-related decisions and information are distributed to the ISSOs and other appropriate persons.	SI-5
4.9.j	Component SOCs shall report operationally to their respective Component CISO. Each CISO shall exercise oversight over their Component's information security operations functions, including the Component SOCs.	IR-1
4.9.k	The DHS SOC shall report operationally to the DHS CISO.	---

Policy ID	DHS Policy Statements	Relevant Controls
4.9.l	The NOC/SOC shall be under the direction of a Government employee who shall be present at all times.	

4.9.1 Security Incidents and Incident Response and Reporting

Policy ID	DHS Policy Statements	Relevant Controls
4.9.1.a	Components shall establish and maintain a continuous 24x7 incident response capability.	IR-1
4.9.1.b	Component SOCs shall report significant incidents to the DHS SOC via EOCOnline (https://eoconline.dhs.gov) as soon as possible but not later than one hour after the DHS SOC report. Other means of reporting, such as calling 1-877-DHS1NET (1-877-347-1638) or emailing DHS.SOC@dhs.gov are acceptable, but the Component shall positively verify that notification, if not submitted via EOConline, 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, via HSDN or Secure Terminal Equipment (STE) cleared to the level commensurate with the incident being reported, as soon as possible but not later than one hour after the DHS SOC report. Subsequent updates and status reports shall be provided to the HSDN SOC and to the DHS SOC via secure email 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://eoconline.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

Policy ID	DHS Policy Statements	Relevant Controls
4.9.1.f	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.g	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.h	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.i	The DHS SOC shall respond to cyber-attacks, events, and incidents pertaining to DHS assets. When an external organization is involved, the DHS SOC will coordinate with the external organization through US-CERT, except in time-sensitive cases where a response requires direct contact with the external organization.	IR-1
4.9.1.j	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 "Incident Response," Attachment F to the *DHS 4300A Sensitive Systems Handbook*.	IR-7 IR-8
4.9.1.k	Components shall develop and publish internal computer security incident response plans and incident handling procedures, and make copies available to the DHS SOC upon request. Each procedure shall include a detailed Configuration Management (CM) process for modification of security device configurations.	IR-1
4.9.1.l	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.m	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.n	The DHS CISO shall determine the frequency and content of security incident reports.	IR-6
4.9.1.o	The Component SOC shall report incidents only to the DHS SOC and to no other external agency or organization.	IR-6
4.9.1.p	The DHS CISO shall publish Incident Response Testing and Exercise scenarios as required.	IR-1

Policy ID	DHS Policy Statements	Relevant Controls
4.9.1.q	The Component CISO for each Component that provides an incident response capability shall ensure Incident Response Testing and Exercises are conducted annually in coordination with the DHS CISO.	IR-3

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 (LE) 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 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 counterintelligence (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

4.10 Documentation

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

Policy ID	DHS Policy Statements	Relevant Controls
4.10.b	System Owners shall update system documentation annually or whenever significant changes occur. Changes that may require updates include: • 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

4.11 Information and Data Backup

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.	---
4.11.c	Components shall implement and enforce backup procedures as part of their contingency planning.	CP-9
4.11.d	All portable backup media in transit shall use encryption in compliance with Section 5.5.1 of this Policy Directive.	CP-9
4.11.e	Components shall follow the procedures established by DHS Management Directive (MD) 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, for the transportation or mailing of backup media.	MP-5

Policy ID	DHS Policy Statements	Relevant Controls
4.11.f	Backup media shall be shipped using an accountable delivery service (e.g. U.S. Postal Service First Class Mail, Federal Express, United Parcel Service) and shall be properly inventoried.	CP-9, MP-5
4.11.g	Every information system shall have a documented chain of custody process for the handling and transportation of portable backup media.	MP-5

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 information and may also be connected to data communications networks.

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
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

Policy ID	DHS Policy Statements	Relevant Controls
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 information shall have the inbound dial in capabilities disabled.	AC-17

5.0 TECHNICAL POLICIES

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

5.1 Identification and Authentication

Policy ID	DHS Policy Statements	Relevant Controls
5.1.a	Components shall ensure that user access is controlled and limited based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.	IA-1, IA-2
5.1.b	For information systems requiring authentication controls, Components shall ensure that the information system is configured to require that each user be authenticated before information system access occurs.	IA-1, IA-2
5.1.c	For systems with low impact for the confidentiality security objective, Components shall disable user identifiers after 90 days of inactivity; for systems with moderate and high impacts for the confidentiality security objective, Components shall disable user identifiers after 45 days of inactivity. This policy applies to anyone who is granted account access to any network, system, or application in use in the Department.	IA-4
5.1.d	Department of Homeland Security (DHS) users shall not share identification or authentication materials of any kind, nor shall any DHS user allow any other person to operate any DHS system by employing the user's identity.	IA-5
5.1.e	All user authentication materials shall be treated as sensitive material and shall carry a classification as high as the most sensitive information 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 HSPD-12 [9].	IA-2

[9] *HSPD = Homeland Security Presidential Directive*

Policy ID	DHS Policy Statements	Relevant Controls
5.1.g	Personal Identification Verification (PIV) credentials or alternative solutions that provide NIST SP 800-63-2 Level of Assurance (LOA) 4 of the user's identity shall be used as the primary means of logical authentication for DHS sensitive systems. Per NIST SP 800-63-2, "Electronic Authentication Guideline," a username, password and single factor one-time password (e.g. RSA SecurlD) is not LOA 4-compliant.	---
5.1.h	Mandatory smart card logon shall be implemented by means of Identity (user) Based Enforcement	IA-2
5.1.i	Privileged network users shall use the DHS HSPD-12 credential for authentication to all DHS Privileged network user accounts.	IA-2
5.1.j	Only approved DHS Privileged Network User Management solutions shall be employed. A waiver request will be required for use of any other solution(s).	---
5.1.k	Systems shall prompt privileged users to enter the PIV PIN to initiate an encrypted authenticate session.	---
5.1.l	Password authentication shall be disabled for all accounts. Where applicable, all password-based authentication modules shall be disabled. This policy applies to all IP-addressable devices.	---
5.1.m	All system access shall be by use of the user's PIV card.	IA-2
5.1.n	Users shall report lost, stolen, or inadvertently destroyed PIV cards to the Help Desk, who shall supply for logon a temporary password account that shall expire within 5 days of creation.	---
5.1.o	Users shall report forgotten or misplaced PIV cards to the Help Desk, who shall supply for logon a temporary password account that shall expire 24 hours after creation.	---

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.

Guidance for the creation of strong passwords is available in Section 5.1.1.1 of the *DHS 4300A Sensitive Systems Handbook*.

Policy ID	DHS Policy Statements	Relevant Controls
5.1.1.a	In those systems where user identity is authenticated by password, Components shall ensure that DHS information systems follow the hardening guides for operating systems (found at http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Pages/sscg.aspx) and the configuration guides for applications promulgated by the DHS CISO to determine and enforce appropriate measures to ensure that strong passwords are used. In the absence of appropriate password complexity guidance, 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
5.1.1.f	Components shall ensure that all passwords are stored in encrypted form.	IA-5
5.1.1.g	Systems shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	IA-6

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.

5.2 Access Control

Policy ID	DHS Policy Statements	Relevant Controls
5.2.a	Components shall implement access control policy and procedures that provide protection from unauthorized alteration, loss, unavailability, or disclosure of information.	AC-1
5.2.b	Access control shall follow the principles of least privilege and segregation of duties and shall require users to use unique identifiers. *Social Security Numbers shall not be used as login IDs*.	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
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).	---

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 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 *account* after three consecutive failed logon attempts.	AC-7

Policy ID	DHS Policy Statements	Relevant Controls
5.2.1.b	The automatic lockout period for accounts locked due to failed login attempts shall be set for 20 minutes.	AC-7
5.2.1.c	Components shall establish a process for manually unlocking accounts prior to the expiration of the 20 minute period, after sufficient user identification is established. This may be accomplished through the help desk.	AC-7

5.2.2 Automatic Session Termination

The term *session* refers to a connection between a terminal device (workstation, laptop, mobile device) and a networked application or system. The term also refers to accessing an application or system such as a database or networked application through the DHS network. The term does not apply to a direct connection to a DHS network, as when authenticating from a device that is directly connected to a 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 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 be automatically terminated after 60 minutes of inactivity.	SC-10

5.2.3 Warning Banner

The DHS CISO stipulates that a warning banner statement be displayed on all DHS systems during logon. The most current language can be found on the DHS CISO Web page.

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

The use of the warning banner serves as a reminder to all users that the computers they are accessing are Government computers.

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

5.3 Auditing

Policy ID	DHS Policy Statements	Relevant Controls
5.3.a	Audit records shall be sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. Audit records shall be reviewed as specified in the SP. The audit record shall contain at least the following information: - Identity of each user and device accessing or attempting to access the system - Time and date of the access and the logoff - Activities that might modify, bypass, or negate information security safeguards - Security-relevant actions associated with processing - All activities performed using an administrator's identity When the technology is available, Components shall ensure implementation of enterprise auditing and recording of sessions (keystroke and graphical).	AU-3, AU-12
5.3.b	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 to the Component CISO/ISSM.	AU-6
5.3.c	Components shall ensure that their audit records and audit logs are protected from unauthorized access, modification, or destruction.	AU-9

Policy ID	DHS Policy Statements	Relevant Controls
5.3.d	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 90 days. Audit trail records shall be preserved for a period of three years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease. Components shall allocate appropriate audit record storage capacity in accordance with these requirements.	AU-4, AU-11
5.3.e	Components shall evaluate the system risks associated with extracts of PII from databases. If the risk is determined to be sufficiently high, a procedure shall be developed for logging computer-readable data extracts. If logging these extracts is not possible, this determination shall be documented, and compensating controls identified in the SP.	AU-1, AU-2, AU-3, PM-9
5.3.f	Component Security Operations Centers (SOC) shall implement both general and threat-specific logging.	AU-1, AU-2
5.3.g	Components shall ensure that information systems alert the Component or DHS SOC in the event of an audit processing failure and overwrite the oldest audit records, if an analysis of the mission needs and the risk to the system preclude system shutdown.	AU-5
5.3.h	Components shall ensure that information systems provide an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents b. Does not alter the original content or time ordering of audit records. (This capability could be as simple as a text editor that allows the administrator to produce a sorted text file, or extract data from an audit log.)	AU-7
5.3.i	Components shall ensure that audit logs employ a consistent time stamp across all systems.	AU-8

5.4 Network and Communications Security

5.4.1 Remote Access and Dial-In

Remote access technology allows trusted employees to access DHS networks by dialing in via modem or accessing the DHS network via the Internet. This allows mobile employees to stay in touch with the home office while traveling. There are significant security risks, however, associated with remote access and dial-in capabilities. Proper procedures can help mitigate these risks.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.1.a	Data communication connections via 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 devices 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 authorized user. Remote access solutions shall comply with the encryption requirements of FIPS 140-2, *Security Requirements for Cryptographic Modules*. See Section 3.14 of this Policy Directive, "Privacy and Data Security" for additional requirements involving remote access of PII.	AC-4, AC-17, AU-2, SC-7, SC-8,
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,
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 in the SP.	---

5.4.2 Network Security Monitoring

Security monitoring, detection, and analysis are key functions and are critical to maintaining the security of DHS information systems. 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.

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 as well as properly identified and categorized information of third parties when required by the Department or a Component. Here *rights* 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
5.4.2.d	Components shall establish monitoring scope at least as comprehensive and stringent as described in Attachment F, "Incident Response," to *DHS 4300A Sensitive Systems Handbook*.	---

5.4.3 Network Connectivity

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

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 the Trusted Internet Connection (TIC) 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 (SLA) or Interconnection Security Agreements (ISA).	CA-3
5.4.3.c	Components shall document all interconnections to the DHS OneNet with an ISA signed by the OneNet AO and by each appropriate AO. Additional information on ISAs is published in, "Preparation of Interconnection Security Agreements," Attachment N to the *DHS 4300A Sensitive Systems Handbook.*	CA-3
5.4.3.d	ISAs shall be reissued every three 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 Modernization Act of 2014 (FISMA) self-assessment.	CA-3
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, *security policies* refers to the set of rules that controls a system's working environment, and not to DHS information security policy). ISAs shall be signed by 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

Policy ID	DHS Policy Statements	Relevant Controls
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 Framework.	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 Change Control Board (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 an SLA or contract, and the risks have been assessed and accepted by all involved AOs.	CA-3
5.4.3.n	Granting the ability to log into one DHS system through another DHS system (such as through OneNet trust) does not require an ISA, when the requirements from Section 5.4.3.m are met.	---
5.4.3.o	The information system shall protect the authenticity of communications sessions.	SC-23
5.4.3.p	For systems with high or moderate impact for any of the FIPS 199 security objectives, system resource sharing shall be limited to an operational need. The information system shall prevent unauthorized and unintended information transfer via shared system resources. All information transfer is limited to that information which has been included in the SP and has been analyzed in the risk assessment for the system.	SC-4

5.4.4 Firewalls and Policy Enforcement Points

Policy Enforcement Points (PEP) separate Trust Zones as defined in the DHS Security Architecture. Boundary protection between DHS and external networks is implemented by firewalls at the TICs and other approved direct system interconnections. DHS TICs are provided by OneNet and monitored by the DHS SOC. Component SOCs may protect DHS-internal boundaries across Trust Zones.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.4.a	Components shall restrict physical access to firewalls and PEPs 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.	--
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 *all* applied policies and controls are operating as intended.	SC-7
5.4.4.e	Component SOCs shall ensure that reports on information security operations status and incident reporting are provided to the DHS CISO as required by this Policy Directive.	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 prevent traffic as directed by the DHS CIO.	SC-7
5.4.4.j	The DHS SOC shall oversee all enterprise PEPs.	---
5.4.4.k	Components shall ensure each information system separates user functionality (including user interface services) from information system management functionality. User interface services (e.g., public web pages) are separated physically and logically from information storage and management services (e.g., database management). The separation may be accomplished through the use of different computers, different central processing units, different instances of operating systems, different network addresses, or a combination of these or other techniques. (Isolation of a public Web page in a Demilitarized Zone (DMZ) is an example of this separation.)	SC-2, SC-32
5.4.4.l	For high impact systems, the information system isolates security functions from other functions.	SC-3

Policy ID	DHS Policy Statements	Relevant Controls
5.4.4.m	For high impact systems, the information system shall fail to a known-state while preserving system state information in failure.	SC-24
5.4.4.n	For high impact systems, the information system shall: a. Verify the correct operation of related security functions b. Perform this verification upon reboot, or command by user with appropriate privilege c. Notify an authorized person of failed security verification tests d. Provide for a Component-defined action (e.g., shut the information system down, or restart the information system) when anomalies are discovered.	SI-6

5.4.5 Internet Security

Policy ID	DHS Policy Statements	Relevant Controls
5.4.5.a	Any direct connection of OneNet, DHS networks, or DHS mission systems to the Internet or to extranets shall occur through DHS TIC PEPs. The Public Switched Telephone Network (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
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

Policy ID	DHS Policy Statements	Relevant Controls
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
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.	---

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.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.6.a	Components shall correctly secure, install, and configure the underlying email operating system.	---
5.4.6.b	Components shall correctly secure, install, and configure mail server software.	---
5.4.6.c	Components shall secure and filter email content.	---
5.4.6.d	Components shall deploy appropriate network protection mechanisms, such as: - Firewalls - Routers - Switches - Intrusion detection systems	---
5.4.6.e	Components shall secure mail clients.	---

Policy ID	DHS Policy Statements	Relevant Controls
5.4.6.f	Components shall conduct mail server administration in a secure manner. This includes: - Performing regular backups - Performing periodic security testing - Updating and patching software - Reviewing audit logs at least weekly	---
5.4.6.g	The DHS email gateway Steward shall provide email monitoring for malware activity at the gateway.	SI-3
5.4.6.h	The DHS email gateway Steward shall provide email monitoring for spam at the gateway.	SI-8
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.	---
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.	
5.4.6.l	Only Government email accounts shall be used to perform Government business.	

5.4.7 Personal Email Accounts

Policy ID	DHS Policy Statements	Relevant Controls
5.4.7.a	The use of Internet Webmail (e.g., Gmail, Yahoo, AOL) or other personal email accounts is not authorized over DHS furnished equipment or network connections.	---

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.

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.

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://eoconline.dhs.gov).	SI-5
5.4.8.e	When vulnerability assessment responsibilities encompass more than one Component, Component CISOs/ISSMs shall coordinate with the relevant Component SOC and the DHS SOC.	RA-3, AU-2Re
5.4.8.f	The DHS SOC shall be notified before any ISVM scans are run.	RA-3, 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

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.

5.4.9 Peer-to-Peer Technology

Policy ID	DHS Policy Statements	Relevant Controls
5.4.9.a	Peer-to-peer software technology is prohibited on any DHS information system.	CM-7, CM-10

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.

5.5.1 Encryption

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

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

5.5.2 Public Key Infrastructure

A Public Key Infrastructure (PKI) is an architected set of systems and services that provide a foundation for enabling the use of public key cryptography. This is necessary in order to implement strong security services and to allow the use of digital signatures.

The principal Components of a PKI are the public key certificates, registration authorities (RA), certification authorities (CA), directory, certificate revocation lists (CRL), and a governing certificate policy.

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.a	**DHS shall implement two distinct PKIs:** **DHS Federal PKI (FPKI):** DHS shall implement a DHS Public Key Infrastructure (PKI) that is part of the FPKI to facilitate the use of PKI within DHS, and to facilitate the interoperable use of PKI between DHS and its external mission and business partners, such as other Federal agencies; state, local and tribal governments; public and private sector entities; and U.S. citizens. **DHS Internal Use NPE PKI:** At the DHS Enterprise-level, a single DHS Enterprise Internal Use Non-Person Entity (NPE) PKI may be implemented to issue certificates to DHS NPEs to support NPE-to-NPE authentication across DHS networks, where the certificates have no external relying parties. At the DHS Component-level, a DHS Component may implement one or more DHS Internal Use Non-Person Entity (NPE) PKIs for use solely by that Component to issue certificates to that Component's NPEs to support NPE-to-NPE authentication on that Component's networks, where the certificates have no external relying parties.	SC-17
5.5.2.b	The DHS CISO shall be the DHS PKI Policy Authority (PKIPA) to provide PKI policy oversight for all DHS PKIs. **DHS FPKI:** A detailed description of DHS PKIPA roles and responsibilities is provided in the Registration Practice Statement for the DHS Principal Certification Authority. **DHS Internal Use NPE PKI:** A detailed description of DHS PKIPA roles and responsibilities is provided in the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines.	SC-17
5.5.2.c	The DHS CISO shall represent DHS on the Federal PKI Policy Authority (FPKIPA).	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.d	The DHS PKIPA shall appoint a PKI Management Authority (PKIMA) to provide management and operational oversight for all DHS PKIs. **DHS FPKI:** A detailed description of DHS PKIMA roles and responsibilities is provided in the Registration Practice Statement for the DHS Principal Certification Authority. **DHS Internal Use NPE PKI:** A detailed description of DHS PKIMA roles and responsibilities is provided in the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines.	SC-17
5.5.2.e	**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 Infrastructure (PKI) X.509 Certificate Policy approved by the Department of the Treasury Policy Management Authority (PMA). **DHS Internal Use NPE PKI:** DHS Internal Use NPE PKIs shall be governed by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines approved by the DHS PKIPA.	SC-17
5.5.2.f	**DHS FPKI:** DHS shall have a single DHS Principal CA (i.e. named 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.	SC-17
5.5.2.g	**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. **DHS Internal Use NPE PKI:** A single DHS Enterprise Internal Use Non-Person Entity (NPE) PKI may be implemented. A DHS Component may implement one or more DHS Internal Use NPE PKIs. Each PKI shall be a hierarchical PKI with one or more levels. • For a single-level hierarchy, the PKI shall consist of a single self-signed Internal Use NPE CA. • For a two-level hierarchy, the PKI shall consist of a single self-signed Internal Use NPE Root CA at the top level, and one or more Internal Use NPE CAs that are each directly subordinated to the Internal Use	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
	NPE Root CA. • Additional Internal Use NPE CAs may be directly subordinated to an existing subordinate Internal Use NPE CA, thereby adding an additional level to the hierarchy. The requirements and process for implementing a DHS Enterprise Internal Use Non-Person Entity (NPE) Root and Subordinate CAs, and for implementing a DHS Component Internal Use NPE Root and Subordinate CAs shall be specified in the NPE PKI Configuration and Operation Practices Guidelines.	
5.5.2.h	**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. The U.S. Common Policy Root CA is cross-certified with the Federal Bridge CA at the high, medium hardware, and medium assurance levels. **DHS Internal Use NPE PKI:** If a DHS Internal Use NPE PKI consists of a single NPE CA, the CA shall be self-signed and function as its own trust anchor. If a DHS Internal Use NPE PKI is a multi-level hierarchical PKI, with a Root and subordinate CAs, the trust path from the subordinate CAs shall resolve to the Root CA as the PKI's trust anchor. A request to implement trust relationships between DHS Component Internal Use Non-Person Entity (NPE) PKIs, or between the DHS Enterprise Internal Use Non-Person Entity (NPE) PKI and a DHS Component Internal Use Non-Person Entity (NPE) PKI must be submitted to the DHS PKIMA for review and approved by the DHS PKIPA.	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.i	**DHS FPKI:** The DHS Principal CA shall operate under an X.509 Certification Practice 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. DHS shall operate two Registration Authorities for the DHS Principal CA (PC4). 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. 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. **DHS Internal Use NPE PKI:** DHS Internal Use NPE CAs shall operate under the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines, which shall be approved by the DHS PKIPA.	SC-17
5.5.2.j	**DHS FPKI:** The DHS PKIMA shall ensure that the DHS PCA Registration Authority (DHS PCA RA) operates in compliance with the RPS. The DHS PIV Card Issuer (PCI) Organization Identity Management Official (DHS OIMO) shall ensure that the DHS PCA PIV Registration Authority (DHS PCI PIV RA) operates in compliance with the RPS. **DHS Internal Use NPE PKI:** The DHS PKIMA shall ensure that every DHS Internal Use NPE CA operates in compliance with the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines.	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.k	**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. **DHS Internal Use NPE PKI:** Every DHS Internal Use NPE CA shall undergo regular PKI compliance assessments as required by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines. The assessment report, findings, and Plans of Action and Milestones (POA&Ms) that address the deficiencies found, shall be provided to the DHS PKIPA and DHS PKIMA.	SC-17
5.5.2.l	**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. **DHS Internal Use NPE PKI:** Every DHS Internal Use NPE CA (Root and Subordinates) shall archive records as required by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines.	SC-17
5.5.2.m	**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.	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.n	**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. 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, medium Hardware, PIV-I, or high assurance level). **DHS Internal Use NPE PKI:** DHS Enterprise Internal Use Non-Person Entity (NPE) CAs shall only issue authentication certificates to DHS NPEs (i.e**.,** hardware devices and systems) when all of the following conditions apply: • There are no relying parties for the certificates external to DHS • The certificates shall only be used for authentication • The certificates are explicitly authorized to be issued by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines 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: • There are no relying parties for the certificates external to the DHS Component • The certificates shall only be used for authentication • The certificates are explicitly authorized to be issued by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines A DHS Enterprise Internal Use NPE Root CA may issue a CA certificate to subordinate a DHS Enterprise Internal Use NPE CA to the Root CA. A DHS Component Internal Use NPE Root CA may issue a CA certificate to subordinate a DHS Component Internal Use NPE CA for that Component to the Root CA. A DHS Enterprise Internal Use NPE CA may issue a CA certificate to subordinate a DHS Enterprise Internal Use NPE CA to itself. A DHS Component Internal Use NPE CA may issue a CA certificate to subordinate a DHS Component Internal Use NPE CA for that Component to itself.	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.o	**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. Only the DHS Principal CA shall issue certificates to DHS NPEs, i.e., hardware devices, systems and applications, when any of the following conditions apply: • 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 information, and • The certificates are not explicitly authorized to be issued by DHS Internal Use NPE CAs in the DHS X.509 Internal Use NPE Certificate Policy.	SC-17
5.5.2.p	**DHS FPKI:** The Treasury Root CA shall be used by Relying Parties in DHS as the trust anchor for the validation of certificates issued by the DHS Principal CA (DHS CA4). The U.S. Common Root CA shall be used by Relying Parties external to DHS as the trust anchor for the validation of certificates issued by the DHS Principal CA (DHS CA4). The U.S. Common Root CA shall also be used by Relying Parties in DHS as the trust anchor for the validation of certificates issued by CAs external to DHS.	SC-17
5.5.2.q	The use by DHS of any non-DHS PKI provider for CA or PKI services is prohibited unless approved by the DHS CISO on a case-by-case basis.	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.r	**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. Certificates issued by test, pilot, third party, self-signed or other CAs shall not be used to protect sensitive information, or to authenticate to DHS operational systems containing sensitive information. **DHS Internal Use NPE PKI:** Certificates issued by DHS Internal Use NPE CAs, shall only be used for authentication.	SC-17
5.5.2.s	**DHS FPKI:** For an external-facing DHS web server, where the browsers used by external relying parties are unable to validate DHS Secure Socket Layer/Transport Layer Security (SSL/TLS) certificates, the use of an 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.	SC-17
5.5.2.t	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. 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.	SC-17
5.5.2.u	**DHS FPKI:** 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. DHS Components shall manage the content of installed product's trust stores, including: • Leveraging automated management, such as with Microsoft Group Policy Objects (GPOs) • Removing all certificates that have passed their expiration date • Removing all certificates that are no longer trusted • Removing all certificates that are no longer required	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.v	**DHS FPKI:** 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: • SHA 1 and SHA 256 • RSA 1024 and 2048 • AES 128 and 256 Whenever possible, they should also support use of the following algorithms and associated key sizes, to ensure future interoperability across the Federal PKI and PKIs cross-certified with the Federal Bridge Certification Authority. • SHA 384 and 512 • RSA 3072 • Elliptic Curve 224, 256, and 384 • ECDSA 224 and 256 *(Note: Older algorithms and smaller key sizes (e.g., SHA 1 and RSA 1024) should continue to be supported since they may be required to validate digital signatures executed in the past and to decrypt objects encrypted in the past using the older algorithms and key sizes.)*	SC-17

5.5.3 Public Key/Private Key

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

Policy ID	DHS Policy Statements	Relevant Controls
5.5.3.a	**DHS FPKI:** Any key pair and associated certificate issued to a human subscriber to support digital signature use, shall not be used to support any other use.	SC-12
5.5.3.b	**DHS FPKI:** A single public/private key pair and its associated certificate issued to an NPE may be used for signing (including authentication), key management (for encryption), or both. Device certificates shall not assert non-repudiation.	SC-12

Policy ID	DHS Policy Statements	Relevant Controls
5.5.3.c	**DHS FPKI:** An 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	**DHS FPKI:** 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	**DHS FPKI:** 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	**DHS FPKI:** Subscriber private keys shall not be used by more than one entity, with the following exceptions: • Authorized members of a Group Subscriber, may use the Group's private keys. • Multiple systems or devices in a high availability configuration may use a single Key pair providing the Subject Alternative Name (SAN) field within the SSL certificate identifies all of the devices with which the key is to be shared.	SC-12

Policy ID	DHS Policy Statements	Relevant Controls
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

5.6 Malware Protection

Policy ID	DHS Policy Statements	Relevant Controls
5.6.a	Component CISOs/ISSMs shall establish and enforce Component-level malware protection control policies.	SI-3
5.6.b	Components shall implement a defense-in-depth strategy that: - Installs anti-malware software on desktops and servers - Configures anti-malware software on desktops and servers to check all files, downloads, and email - Installs updates to anti-malware 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

5.7 Product Assurance

Policy ID	DHS Policy Statements	Relevant Controls
5.7.a	Information Assurance (IA) shall be considered a requirement for all systems used to input, process, store, display, or transmit sensitive or national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated 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	*Strong preference* shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting sensitive information) that have been evaluated and validated, as appropriate, in accordance with the following: - The National Institute of Standards and Technology (NIST) FIPS validation program - The NSA/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program - The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement	---
5.7.c	The evaluation and validation of COTS IA and IA-enabled products shall be conducted by 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
5.7.f	For systems with moderate or high impact for the integrity security objective, Components shall perform a risk-based analysis to determine any data inputs that are critical to the system mission or the correct handling of the security controls, which should be checked for accuracy, completeness, and validity of the information as close to the input point (e.g., user interface) as possible. Inputs that go through interpreters should be prescreened.	SI-10
5.7.g	For systems with moderate or high impact for the integrity security objective, the information system shall check the validity of these Component-defined information inputs.	SI-10

Policy ID	DHS Policy Statements	Relevant Controls
5.7.h	For systems with moderate or high impact for any of the FIPS 199 security objectives, Components shall perform a risk-based analysis to determine what error conditions should be identified and how expeditiously they should be handled.	SI-11
5.7.i	For systems with moderate or high impact for any of the FIPS 199 security objectives, the information system shall generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. Error messages shall be revealed only to authorized personnel.	SI-11

5.8 Supply Chain

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

Policy ID	DHS Policy Statements	Relevant Controls
5.8.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 800-161 controls as tailored specifically to the security objective at the determined impact level.	SA-12
5.8.b	Components shall implement NIST SP 800-161security controls, using the FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems methodology, based on the FIPS 199 impact level established for each separate security objective (confidentiality, integrity, availability).	SA-12

5.8.1 Business Impact

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

Policy ID	DHS Policy Statements	Relevant Controls
5.8.1.a	A Business Impact Assessment (BIA) shall be used to determine the level of risk introduced to the system by the supply chain and whether supply chain threats introduce sufficient risk to require the implementation of countermeasures.	SA-12

5.8.2 Supply Chain Risk Management Plans

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

Policy ID	DHS Policy Statements	Relevant Controls
5.8.2.a	DHS Components shall develop, document, and disseminate requirements for all programs under their control to develop a plan to address supply chain risk.	SA-1 SA-12
5.8.2.b	DHS Components shall assess supply chain threats for risks associated with all hardware, software, and services acquired or projected to be acquired with the goal of mitigating those risks to the greatest extent possible.	SA-12

6.0 DOCUMENT CHANGE REQUESTS

Changes to *DHS Sensitive Systems Policy Directive 4300A* and to the *DHS 4300A Sensitive Systems Handbook* may be requested in accordance with Section 1.9, Changes to Policy.

7.0 QUESTIONS AND COMMENTS

For clarification of DHS information security policies or procedures, contact the DHS Director for Information Systems Security Policy at infosecpolicy@hq.dhs.gov.

APPENDIX A ACRONYMS AND ABBREVIATIONS

ACRONYM	MEANING
3DES	Triple Data Encryption Standard
3PAO	Third Party Assessors
AES	Advanced Encryption Standards
AIS	Automated Information System
A-Number	Alien Registration Number
AO	Authorizing Official
ARB	Acquisition Review Board
ASCII	American Standard Code for Information Interchange
ATO	Authority to Operate
BI	Background Investigation
BIA	Business Impact Assessment
BLSR	Baseline Security Requirements
CA	Certification Authority
CAC	Common Access Card
CBP	Customs and Border Protection
CCB	Change Control Board
CCE	Common Configuration Enumeration
CD	Compact Disc
CFO	Chief Financial Officer
CI	Counterintelligence
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
CMA	Computer Matching Agreements

ACRONYM	MEANING
CMG	Core Management Group
CMP	Configuration Management Plan
CNSS	Committee on National Security Systems
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan Continuity of Operations Planning
COTS	Commercial-off-the-shelf
CP	Contingency Plan Contingency Planning
CPE	Common Platform Enumeration
CPIC	Capital Planning and Investment Control
CRE	Computer-Readable Extract
CRL	Certificate Revocation List
CSO	Chief Security Officer
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNSSEC	Domain Name System Security Extensions
DOD	Department of Defense
EA	Enterprise Architecture
EAB	Enterprise Architecture Board
EMSG	Email Security Gateway
EO	Executive Order
EOC	Enterprise Operations Center 2,
ESSA	Enterprise System Security Agreement
ESSWG	Enterprise Services Security Working Group

ACRONYM	MEANING
EV	Extended Validation
FAM	Foreign Affairs Manual
FBCA	Federal Bridge Certification Authority
FDCC	Federal Desktop Core Configuration
FedRAMP	Federal Risk and Authorization Management Program
FEMA	Federal Emergency Management Agency
FICAM	Federal Identity, Credentialing, and Access Management
FIPS	Federal Information Processing Standard
FIPPS	Fair Information Practice Principles
FISMA	Federal Information Security Modernization Act of 2014
FLETC	Federal Law Enforcement Training Center
FNVMS	Foreign National Vetting Management System
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FPKI	Federal Public Key Infrastructure
FPKI PA	Federal PKI Policy Authority
FTP	File Transfer Protocol
FYHSP	Future Years Homeland Security Program
GPEA	Government Paperwork Elimination Act
GSA	General Services Administration
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
HQ	Headquarters
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

ACRONYM	MEANING
	Information Assurance
IACS	Information Assurance Compliance System
IATO	Interim Authority to Operate
ICAM	Identity, Credentialing, and Access Management
ICCB	Infrastructure Change Control Board
ICE	Immigration and Customs Enforcement
IDS	Intrusion Detection System
IOC	Initial Operating Capability
IPS	Intrusion Prevention System
IPT	Integrated Project Team
IR	Infrared
IRB	Investment Review Board
ISA	Interconnection Security Agreement
ISMS	Integrated Security Management System
ISO	Information Security Office
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISVM	Information System Vulnerability Management
IT	Information Technology
JAB	Joint Authorization Board
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
LE	Law Enforcement
LMR	Land Mobile Radio
MA	Major Application
MBI	Moderate Risk Background Investigation
MD	Management Directive
MMS	Multimedia Messaging Service
NARA	National Archives and Records Administration

ACRONYM	MEANING
NCCIC	National Cybersecurity and Communications Information Center
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NPPD	National Protection and Programs Directorate
NPE	Non-person Entity
NSA	National Security Agency
NSS	National Security System(s)
NTP	Network Time Protocol
OA	Ongoing Authorization
OCIO	Office of the Chief Information Officer
OCSO	Office of the Chief Security Officer
OCSP	Online Certificate Status Protocol
OID	Object identifier
OIG	Office of Inspector General
OIMO	Organization Identity Management Official
OMB	Office of Management and Budget
OPA	Office of Public Affairs
OPM	Office of Personnel Management
ORMB	Operational Risk Management Board
OTAR	Over-The-Air-Rekeying
PA	Policy Authority
PAdES	PDF Advanced Electronic Signatures
P-ATO	Provisional Authority to Operate
PBX	Private Branch Exchange
PCI	PIV Card Issuer
PCS	Personal Communications Services
PDVAL	Path Development and Validation
PEP	Policy Enforcement Point

ACRONYM	MEANING
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
PIV-I	Personal Identity Verification - Interoperable
PKI	Public Key Infrastructure
PKI PA	PKI Policy Authority
PKI MA	PKI Management Authority
PM	Program Manager
PMA	Policy Management Authority
PMO	Program Management Office
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
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFID	Radio Frequency Identification
~~RMS~~	~~Risk Management System~~ Term superseded by IACS
RMF	Risk Management Framework
RPS	Principal Certification Authority
S&T	Science and Technology [Component of DHS]
SA	Security Architecture
SAISO	Senior Agency Information Security Officer
SAN	Subject Alternative Name

ACRONYM	MEANING
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
SEN	Security Event Notification
SLA	Service Level Agreement
SME	Subject Matter Expert
SMS	Short Message Service
SOA	Service Oriented Architecture
SOC	Security Operations Center
SOC CONOPS	Security Operations Center Concept of Operations
SORN	System of Records Notice
SOW	Statement of Work
SP	Special Publication Security Plan
SSH	Secure Shell
SSL	Secure Socket Layer
SSP	Shared Service Provider
Stat.	Statute (refers to a law found in *U.S. Statutes at Large*)
STE	Secure Terminal Equipment
~~TAF~~	~~Trusted Agent FISMA~~ Term superseded by IACS
TFPAP	Trust Framework Provider Adoption Process
TIC	Trusted Internet Connections
TLS	Transport Layer Security
TOS	Terms of Service
TRAL	Trigger Accountability Log
TRM	Technical Reference Model

ACRONYM	MEANING
TS	Top Secret
TS/SCI	Top Secret, Sensitive Compartmented Information
TSA	Transportation Security Administration
UCMJ	Uniform Code of Military Justice
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Service
USGCB	U.S. Government Configuration Baseline
USSS	United States Secret Service
VAT	Vulnerability Assessment Team
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
XML	Extended Markup Language

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 the *National Information Assurance (IA) Glossary*.

TERM	MEANING
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 Modernization Act of 2014 (FISMA) self-assessment requirement.
Authorization Package	The documents submitted to the AO for the Authorization Decision. An Authorization Package consists of: • Security Plan • Security Assessment (SPR) Plan • Security Assessment Report (SAR) • Signed Accreditation Decision Letter/ATO • Contingency Plan (CP) • Contingency Plan Test (CPT)
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 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.

TERM	MEANING
Compensating Control	An internal control intended to reduce the risk of an existing or potential control weakness.
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's, Counselors, and staff, when approved as such by the Secretary), including both Operational Components and Support Components (also known as Headquarters Components). [Source *DHS Lexicon* and DHS Management Directive 112-01]
Computer Security Incident Response Center (CSIRC)	DHS organization that responds to computer security incidents.
Designated Approval Authority (DAA)	Obsolete term; see Authorizing Official (AO).
Digital Signature	Cryptographic process used to assure data object originator authenticity, data integrity, and time stamping for prevention of replay.
Electronic Signature	The process of applying any mark in electronic form with the intent to sign a data object. See also digital signature.
For Official Use Only (FOUO)	The marking instruction or caveat "For Official Use Only" will be used within the DHS community to identify sensitive but unclassifed information that is not otherwise specifically described and governed by statute or regulation. Note: The term *sensitive information* as well as others such as For Official Use Only (FOUO) and Sensitive But Unclassified (SBU) will no longer be used upon implementation of 32 CFR 2002, which will require use of the term Controlled Unclassified Information (CUI).
General Support System (GSS)	A *general support system* (GSS) is an interconnected set of information resources that share common functionality and are under the same direct management control. [expanded definition in the Section 1.4, "Definitions"]
Information and Communications Technology (ICT)	Encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information. Source: NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*

TERM	MEANING
ICT Supply Chain	The organizations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to an organization's customers. Source: National Defense Industry Association (NDIA), *Engineering for System Assurance*, September 2008
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. [Source: Clinger-Cohen Actof 1996 (Public Law 104-106), Division E]
Major Application (MA)	An automated information system (AIS) that requires special attention to security due to the risk and magnitude of harm that can result from the loss, misuse, or unauthorized access to or modification of the information in the application. [Source: OMB Circular A-130] An MA is a discrete application, whereas a GSS may support multiple applications.
Management Controls	The security controls for an information system that focus on the management of risk and the management of information system security.
Operational Controls	The security controls for an information system that are primarily implemented and executed by people (as opposed to being executed by systems).
Operational Risk	The risk contained in a system under operational status. It is the risk that an AO accepts when granting an ATO.

TERM	MEANING
Personally Identifiable Information (PII)	Any information information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual regardless of whether the individual is a United States citizen, legal permanent resident, or a visitor to the United States. [see also Sensitive Personally Identifiable Information]
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.
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.
Privileged Network User	A user that is authorized (and, therefore, trusted) to perform security-relevant functions for purposes including but not limited to network system administration, security policy and procedure management, and system maintenance and controls.
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.

TERM	MEANING
Security Assessment Plan	The security assessment plan and privacy assessment plan provide the objectives for the security and privacy control assessments, respectively, and a detailed roadmap of how to conduct such assessments. These plans may be developed as one integrated plan or as distinct plans, depending upon organizational needs. [per NIST SP 800-53A]
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 DHS SOC coordinates security operations for the DHS enterprise. Each Component also has a SOC that coordinates Component 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.
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. Note: The term *sensitive information* as well as others such as For Official Use Only (FOUO) and Sensitive But Unclassified (SBU) will no longer be used upon implementation of 32 CFR 2002, which will require use of the term Controlled Unclassified Information (CUI).

TERM	MEANING
Sensitive Information	Any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy of individuals, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. Note: The term *sensitive information* as well as others such as For Official Use Only (FOUO) and Sensitive But Unclassified (SBU) will no longer be used upon implementation of 32 CFR 2002, which will require use of the term Controlled Unclassified Information (CUI).
Sensitive Personally Identifiable Information (SPII)	*Sensitive PII* is Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. [see also Personally Identifiable Information]
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	A method used to secure computer systems and/or networks by verifying a user's identity by requiring two-factors in order to authenticate (something you know, something you are, or something you have). Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. [See the discussion of Level 4 assurance in NIST SP 800-63-2, "Electronic Authentication Guideline," (August 2013)]
Supply Chain	A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. Source: CNSSI 4009
Supply Chain Risk Management	A decision making process, usually supported by imperfect or incomplete information, undertaken for the purpose of prioritizing actions related to procuring ICT in support of the mission. Source: DHS SCRM PMO

TERM	MEANING
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	The classic paradigm for authentication systems identifies three factors as the cornerstone of authentication: • *Something you know* (for example, a password or Personal Identification Number (PIN) • *Something you have* (for example, an ID badge or a cryptographic key) • *Something you are* (for example, a fingerprint or other biometric data) The strength of authentication systems is largely determined by the number of factors incorporated by the system. Implementations that use two factors are considered to be stronger than those that use only one factor." A requirement for two of the three factors listed above constitutes two factor authentication.
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.

TERM	MEANING
Visitor	A guest or temporary employee who presents themselves or is presented by a sponsor, for entry for less than 6 months to a secured facility that is not their primary work location. [Source: DHS Lexicon] The visitor is placed in one of two categorizes, either ***escort required*** or ***no escort required***. ***Escort required*** visitors are escorted at all times. ***No escort required*** visitors are granted limited general access to the facility without an escort. Escort procedures for classified areas are indicated in Management Directive 11051 "SCIF Escort Procedures." [Source: DHS Lexicon]
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. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, DC, July 14, 1987
- Computer Security Act of 1987, as amended, codified at 40 U.S.C. 759 , Public Law 100-235
- *Clinger-Cohen Act* of 1996, Public Law 104-106
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191
- E-Government Act of 2002, Public Law 107–347, 116 Stat. 2899, 44 U.S.C. 101
- Freedom of Information Act of 2002, as amended, 5 U.S.C 552, Public Law 93-579
- Intelligence Reform and Terrorism Prevention Act of 2004, 118 Stat. 363
- Federal Information Security Modernization Act of 2014 (FISMA), Public Law 113-283, 128 Stat 3087
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, "Standards of Ethical Conduct for Employees of the Executive Branch"

Executive Orders

- Executive Order 13526, "Classified National Security Information," December 29, 2009
- Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004

Office of Management and Budget Directives

- Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources, Transmittal Letter No. 4," 2010
- OMB Bulletin 06-03, "Audit Requirements for Federal Financial Statements," August 23, 2203
- 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 12-20, "FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," September 27, 2012
- 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 Standards and Guidance

- Intelligence Community Directive (ICD) 503 ""Intelligence Community Information Technology Systems Security: Risk Management, Certification and Accreditation," September 15, 2008
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS), including:
    - NIST FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004
    - NIST FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006
- NIST Information Technology Security Special Publications (SP) 800 series, including:
    - NIST SP 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model," 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, Rev 1, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations," April 2014
    - NIST SP 800-53, Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013, with updates as of January 22, 2015
    - NIST SP 800-53A, Rev 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans," December 2014

- 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 800-63-2, "Electronic Authentication Guideline," August 2013
- NIST SP 800-65, Integrating IT Security into the Capital Planning and Investment Control Process (CPIC)," January 2005
- NIST SP 800-88 Rev 1, "Guidelines for Media Sanitization," December 2014
- 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 (Including updates as of 03-07-2007)
- 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, Rev 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," June 2013
- NIST SP 800-128, "Guide for Security-Focused CM of Information Systems," August 2011
- NIST SP 800-137, "Information Security Continuous Monitoring for Federal Information Systems and Organizations," September 2011
- NIST SP 800-160, "DRAFT Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems," May 2014
- NIST SP 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," April 2015

- NIST IR 7298 Rev 2, "Glossary of Key Information Security Terms," May 2013
- CNSS Instruction No. 1001, "National Instruction on Classified Information Spillage," February 2008
- CNSS Instruction No. 4009 (Revised), "National Information Assurance Glossary," April 2015

Internal Guidance

- Department of Homeland Security Acquisition Regulation (HSAR)
- DHS Management Directives (MD), especially:
  - MD 140-01, "Information Technology Security Program," July 6, 2014
  - MD 11042.1, "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," January 6, 2005
  - MD 102-01a, "Acquisition Management Directive Rev01," January 20, 2010
  - MD 102-01b, "Acquisition Management Directive Rev02," February 21, 2013
  - 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

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.

Version	Date	Description
5.0	March 1, 2007	New policies: 4.1.5.h. Modified policies: 3.10.c, 4.1.1.d, 4.1.5.a,b,f, &g, 4.6.2.d, 4.6.3.f, 5.2.c, 5.4.8.a, 5.6.b. New sections: 4.1.1. Modified sections: 1.2, 1.4.2, 1.4.3, 2.9, 3.12, 4.1 and subsections, 4.6.1–4.6.4, 4.9, 5.2.1. Renumbered sections: 4.1.2–4.1.6, 4.9, 4.10, 4.11, 4.12.
5.1	April 18, 2007	Update based on SOC CONOPS, Final Version 1.4.1, April 6, 2007; Adds DHS Chief Financial Officer – Designated Financial Systems; Updates the term, *Sensitive But Unclassified* to *For Official Use Only*
5.2	June 1, 2007	Updates Sections 2.7, 2.9, 2.12, 3.3, 3.5.1, 3.5.3, 3.6, 3.8, 3.9, 3.10, 3.14, 3.15, 4.1.5, 4.1.6, 4.10, 4.12, 5.1.1, 5.2, 5.3, 5.4.1, 5.4.3, 5.4.4, 5.4.8, 5.5.1, 5.7
5.3	August 3, 2007	Revised policy in Sections 3.5.1 and 5.5.1, and removed Section 3.5.2. Removed Sections 3.11.2 and 3.11.4
5.4	October 1, 2007	Content update, incorporation of change requests
5.5	September 30, 2007	**Section 1.0:** 1.1 – Added text regarding policy implementation and DHS security compliance tool updates. 1.2 – Removed two references from list; deleted "various" from citation of standards. **Section 2.0:** 2.0 – Insert the following after the first sentence in the second paragraph: “Security is an inherently governmental responsibility. Contractors and other sources may assist in the performance of security functions, but a government individual must always be designated as the responsible agent for all security requirements and functions.” 2.3 – Removed parentheses from "in writing." **Section 3.0:** 3.9 – Inserted new policy element “l” regarding CISO concurrence for accreditation. 3.15 – Added text regarding Component CFOs and ISSMs. **Section 4.0:** 4.1.1 – Capitalized “Background,” and added "(BI)." 4.3.1 – Two new elements were added to the policy table. 4.7 – Inserted "where required or appropriate" before the sentence. 4.8.3 – Title changed to “Personally Owned Equipment and Software (not owned by or contracted for by the Government).” 4.8.6 – Included new section regarding wireless settings for peripheral equipment. **Section 5.0:** 5.1c – Changed inactive accounts to “disable user identifiers after forty-five (45) days of inactivity.” 5.1.1 – First sentence of the second paragraph was rewritten to prohibit use of personal passwords by multiple individuals. 5.2.2 – Title changed to “Automatic Session Termination.”
6.0	May 14, 2008	**Global change** “Shoulds” changed to “shalls” throughout the document. Replaced certain instances of “will” with “shall” throughout document to indicate compliance is required. Various changes were made throughout the document to ensure that the 4300A Policy and Handbook align with the 4300B Policy and Handbook. “ISSM” changed to “CISO/ISSM” throughout the document.

Version	Date	Description
		"CPO" changed to "Chief Privacy Officer" throughout the document. "IT Security Program" changed to "Information Security Program" throughout the document." "System Development Life Cycle" changed to "System Life Cycle" and "SDLC" changed to "SLC" throughout the document. **Title Page** Title page of 4300A Policy - Language on the Title Page was reworded. "This is the implementation of DHS Management Directive 4300.1." **Section 1.0** 1.1 – Updated to clarify 90 day period in which to implement new policy elements. 1.2 – Added OMB, NIST, and CNSS references. 1.4 – Added reference and link to Privacy Incident Handling Guidance and the Privacy Compliance documentation. 1.4.2 – Added definition of National Intelligence Information. 1.4.3 – Inserted definition of National Security Information to align with 4300B Policy. 1.4.8.1 – Definition of General Support System was updated. 1.4.8.2 – Definition of Major Application was updated. 1.4.10 – Section was renamed "Trust Zone." 1.4.16 – Inserted new definition for FISMA. 1.5 – Language was updated to increase clarity for financial system owners for waivers and exceptions. **Section 2.0** 2.3 – Added a new responsibility for DHS Chief Information Officer (CIO). 2.4 – Added a new responsibility for Component CIOs. 2.5 - Chief Information Security Officer (CISO) renamed DHS Chief Information Security Officer (CISO). Updated to include privacy-related responsibilities. 2.6 – Added a new section in Roles and Responsibilities called "Component CISO." 2.7 – Updated Component ISSM Role and Responsibilities. 2.8 – Changed name of the section from "Office of the Chief Privacy Officer (CPO)" to "The Chief Privacy Officer". Updated to include privacy-related responsibilities. 2.9 – Added a new role for DHS CSO. 2.10 – Updated to include privacy-related responsibilities. 2.11 - Added privacy-related responsibilities.

Version	Date	Description
		2.12 – Added a new section, “OneNet Steward.” 2.13 – Added a new section, “DHS Security Operations Center (DHS SOC) and Computer Security Incident Response Center (CSIRC).” 2.14 – Added a new section, “Homeland Secure Data Network (HSDN) Security Operations Center (SOC).” 2.16 – Added a new section, “Component-level SOC.” 2.18 – Updated to include privacy-related responsibilities. 2.19 – Last sentence of first paragraph has been updated to say: “ISSO Duties shall not be assigned as a collateral duty. Any collateral duties shall not interfere with their ISSO duties.” 2.20 – Updated to include privacy-related responsibilities. **Section 3.0** 3.9 – Added C&A information for unclassified, collateral classified and SCI systems. Also, prior to DHS Policy table, included sentence regarding C&A. 3.9.b – Language updated to clarify that a minimum impact level of moderate is required for confidentiality for CFO designated financial systems. 3.9.h – New guidance is provided to clarify short term ATO authority. 3.11.1 – Added new section discussing the CISO Board. 3.11.3 – Removed DHS Wireless Security Working Group. 3.14.1 – Added new text defining PII and sensitive PII. At the end of bullet #4, added definition of computer-readable data extracts. Updated 3.14.1.a and 3.14.1.b based on input from the Privacy Office. Added sentence “DHS has an immediate goal that remote access should only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. 3.14.2 - Added new section called "Privacy Threshold Analyses." 3.14.3 - Updated Privacy Impact Assessment Responsibilities table. 3.14.4 - Added new section called "System of Record Notices." **Section 4.0** 4.1.5.c – Updated to address training requirements. 4.1.5.g – Deleted “Training plans shall include awareness of internal threats and basic IT security practices.” 4.1.5.h (now 4.1.5.g) – Updated to include the following sentence: “Components shall account for Contingency Plan Training, and Incident Response Training conducted for Moderate and High IT Systems.” 4.3.1.d – FIPS 140-2 compliance language was updated. 4.8.1.a and 4.8.1.c – Language has been updated to provide clarification of timeout values.

Version	Date	Description
		4.8.2.a – FIPS 140-2 compliance language was updated. 4.8.2.b – Added a new policy element regarding powering down laptops when not in use. 4.9 – Section was renamed "Department Information Security Operations." 4.9, 4.9.1, 4.9.2 – Updated policy elements to support Department security operations capabilities, based on the SOC CONOPS. 4.9.2.b – Updated to say "Components shall obtain guidance from the DHS SOC before contacting local law enforcement except where there is risk to life, limb, or destruction of property." 4.12.a – Added policy element to align with Handbook. **Section 5.0** 5.2.1.a, 5.2.1.b, and 5.2.1.c – Language has been updated to provide clarification of timeout values. 5.2.2 Introductory language, 5.2.2.a, 5.2.2.b, and 5.2.2.c – Language and policy updated to clarify the meaning of a session termination. 5.3.f - Updated to clarify responsibilities of the System Owner regarding computer-readable data extracts. 5.4.1.d – Added sentence "DHS has an immediate goal that remote access should only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access." 5.4.3.a through i – New guidance is provided regarding the preparation of ISAs for interconnections to the DHS OneNetwork. 5.4.3.g – Replaced "interconnect service agreements" with "interconnection security agreements." 5.4.4.f - New guidance is provided regarding internal firewalls. 5.4.5.f – New guidance is provided regarding the use of the RDP protocol. 5.4.6 – Added text "NOTE: Due to many attacks that are HTML-based, please note that DHS will be following the lead of the DoD and moving to text based email." 5.4.8.a – Language updated to reflect that annual vulnerability assessments should be conducted. 5.4.8.f – Policy updated to clarify automated system scanning. 5.5.1.c – Updated element to specify usage of cryptographic modules that "are FIPS 197 compliant and have received FIPS 140-2 validation." 5.5.2.f – Policy updated to clarify hosting of DHS Root CA.
6.1	September 23, 2008	**Global Changes** Replaced all instances of "CISO/ISSM" with "Component CISO/ISSM." Replaced all DHS-related instances of "agency/agency-wide" with "Department/Department-wide." Replaced all instances of "24x7" with "continuous" or "continuously," as

Version	Date	Description
		appropriate. Replaced all instances of "IT security" with "information security." Various minor editorial and grammatical changes were made throughout the document. **Section 1.0** 1.2 – Added reference to E-Government Act of 2002, January 7, 2003. 1.4 – Replaced "National InfoSec Glossary" with "National Information Assurance (IA) Glossary." 1.4.5 – Replaced third sentence with "System vulnerability information about a financial system shall be considered Sensitive Financial Information." 1.5.2 – Added text regarding acceptance of resulting risk by the Component CFO for financial systems. 1.5.3 – Corrected the title and location of Attachment B. Added text regarding PTA requirements. **Section 2.0** 2.1 – Updated to clarify Secretary of Homeland Security responsibilities. 2.2 – Updated to clarify Undersecretaries and Heads of DHS Components responsibilities. 2.3 – Updated to clarify DHS CIO responsibilities. 2.4 – Updated to clarify Component CIO responsibilities. 2.5 – Updated to clarify DHS CISO responsibilities. 2.6 – Updated to clarify Component CISO responsibilities. 2.8 – Moved "The Chief Privacy Officer" section to 2.9. 2.11 – Updated to clarify Program Managers' responsibilities. 2.14 – Updated to clarify HSDN SOC responsibilities. Updated HSDN SOC unclassified email address. 2.19 – Updated to clarify ISSO responsibilities and the assignment of ISSO duties as a collateral duty. 2.20 – Updated to clarify System Owners' responsibilities. 2.23.2 – Updated to clarify DHS CIO responsibilities for financial systems. **Section 3.0** 3.1.e – Replaced "FISMA and OMB requirements" with "FISMA, OMB, and other Federal requirements." 3.1.h – Replaced "maintain a waiver" with "maintain a waiver or exception." 3.14.1 – Included text regarding the type of encryption needed for laptops. 3.14.3 – Included text stating that the PTA determines whether a PIA is conducted.

Version	Date	Description
		3.14.4 – Moved first sentence of second paragraph to be the first sentence of the first paragraph. Included "that are a system of record" after "IT Systems" in the second sentence of the first paragraph. **Section 4.0** 4.3.1.a – Included "locked tape device" in media protection. 4.3.1.d – Updated to clarify that AES 256-bit encryption is mandatory. 4.8.2.a – Updated to clarify that AES 256-bit encryption is mandatory. 4.8.3.c – Included new policy element regarding use of seized IT equipment. 4.8.4.f – Included new policy element regarding management and maintenance of system libraries. 4.8.5.b – Policy updated to clarify limited personal use of DHS email and Internet resources. 4.9 – First paragraph updated to clarify DHS SOC and HSDN SOC responsibilities. 4.9.b – Updated to specify that the HSDN SOC is subordinate to the DHS SOC. 4.9.1 – First two paragraphs updated to clarify relationship between the DHS SOC and the HSDN SOC. 4.9.1.a – Removed the words "Component SOC." 4.9.1.b – Updated to clarify means of communication for reporting significant incidents. 4.9.1.c – Updated to clarify the length of time by which significant HSDN incidents must be reported. 4.9.1.d. – Updated to clarify reporting for HSDN incidents. **Section 5.0** 5.2.d – Replaced "Component CISO/ISSM" with "Component CISO/ISSM or his/her designee." 5.2.1 – Changed "48 hour time period" to "24 hour time period." 5.4.5.g – Included new policy element regarding blocking of specific Internet websites or categories. 5.4.7 – Updated the policy element to prohibit use of Webmail and other personal email accounts. 5.5.1.c – Updated to clarify that AES 256-bit encryption is mandatory. 5.7.d – Included new policy element regarding use of cryptographic modules in order to align with 4300A Handbook. 5.7.e – Included new policy element regarding rollback and journaling for transaction-based systems.
6.1.1	October 31, 2008	5.2.3 – Included new language and a link to the DHS computer login warning banner text on DHS Online.

Version	Date	Description
7.0	July 31, 2009	**General Updates** Added section and reference numbers to policy elements Added NIST 800-53 reference controls to policy elements Added hyperlinks to most DHS references Introduced new terminology Senior Agency Information Security Officer, Risk Executive, and Authorizing Official (AO) – replaces DAA, as per NIST 800-37 and 800-53 Added Appendix A – Acronyms Added Appendix B – Glossary Added Appendix C – References list has been updated and moved to Appendix C. (these are detailed references, an abbreviated list is still found at the beginning of the document) Added Appendix D – Change History (This was moved from the front of the document) **Specific Updates** **Section 1.1 – Information Security Program Policy** – Added the statement, "Policy elements are designed to be broad in scope. Specific implementation information can often be found in specific National Institute for Standards and Technology (NIST) publications, such as NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Systems." **Section 1.4.17-19 – Privacy** – Added definitions for PII, SPII, and Privacy Sensitive Systems **Section 1.5 – Exceptions and Waivers** – Updated this section, clarified policy elements, and consolidated all exceptions and waivers requirements. **Section 1.5.4 – U.S. Citizen Exception Requests** – Updated section to include policy elements: 1.5.4.a – Persons of dual citizenship, where one of the citizenships includes U.S. Citizenship, shall be treated as U.S. Citizens for the purposes of this directive. 1.5.4.b – Additional compensating controls shall be maintained for foreign nationals, based on nations lists maintained by the DHS CSO. **Section 1.6 – Information Sharing and Communication Strategy** – Added policy element: 1.6.a - For DHS purposes, electronic signatures are preferred to pen and ink or facsimile signatures in all cases except where pen & ink signatures are required by public law, Executive Order, or other agency requirements. **Section 1.7 – Changes to Policy** – Updated entire section **Section 2.0 – Roles and Responsibilities** – Reformats entire section. Places emphasis on DHS CISO and Component-level Information Security Roles. Secretary and senior management roles are moved to the end of the section. Some specific areas to note include: **Section 2.1.1 – DHS Senior Agency Information Security Officer** – Introduces this term and assigns duties to DHS CISO **Section 2.1.2 – Chief Information Security Officer** – Adds the following

Version	Date	Description
		responsibilities: - Appoint a DHS employee to serve as the Headquarters CISO - Appoint a DHS employee to serve as the National Security Systems (NSS) CISO **Section 2.1.3 – Component Chief Information Security Officer** – Adds policy element: 2.1.3.b - All Components shall be responsible to the appropriate CISO. Components without a fulltime CISO shall be responsible to the HQ CISO. Adds 4 additional CISOs to the list of Component CISOs: Federal Law Enforcement Training Center Office of the Inspector General Headquarters, Department of Homeland Security The DHS CISO shall also appoint an NSS CISO **Section 2.1.4 – Component Information Systems Security Manager** – Component CISO now works directly with the HQ CISO, rather than with the DHS CISO. **Section 2.1.5 – Risk Executive** – Introduces this term as per NIST. Assigns responsibilities to CISOs (already performing these functions) **Section 2.1.6 – Authorizing Official** – Introduces this term as per NIST. Replaces the term Designated Approval Authority (DAA) **Section 2.2.10 – DHS Employees, Contractors, and Vendors** – Adds the requirement for vendors to follow DHS Information Security Policy **Section 3.2 – Capital Planning and Investment Control** – Adds policy element: 3.2.f – Procurement authorities throughout DHS shall ensure that Homeland Security Acquisition Regulation (HSAR) provisions are fully enforced. **Section 3.3 – Contractors and Outsourced Operations** – Adds policy element: 3.3.g – Procurement authorities throughout DHS shall ensure that Homeland Security Acquisition Regulation (HSAR) provisions are fully enforced. **Section 3.5.2 – Contingency Planning** – Updates and expands entire section. **Section 3.7 – CM** – Adds policy elements Section 3.7.f – If the information system uses operating systems or applications that do not have hardening or do not follow configuration guidance from the DHS CISO, the System Owner shall request an exception, including a proposed alternative secure configuration. Section 3.7.g – Components shall ensure that CM processes under their purview include and consider the results of a security impact analysis when considering proposed changes. **Section 3.9 – Certification, Accreditation, and Security Assessments** – Updates entire section **Section 3.11.1 – CISO Council** – Updates the term from CISO Board

Version	Date	Description
		Section 3.14-3.14.6 – Privacy Sections – Updates all sections pertaining to privacy and privacy information, adds section 3.14.5 – Protecting Privacy Sensitive Systems **Section 3.14.7 – E-Authentication** – Renumbers this section from 3.14.6 (due to adding of privacy section 3.14.5 **Section 3.15 – DHS Chief Financial Officer Designated Systems** – Section renamed from DHS Chief Financial Officer Designated Financial Systems **Section 3.16 – Social Media** – Added Social Media section to provide guidelines and address the Federal Government's (including DHS) use of social media sites (You Tube, Twitter) **Section 4.1.2 – Rules of Behavior** – Added policy element: 4.1.2.b – Components shall ensure that DHS users are trained regarding rules of behavior and that each user signs a copy prior to being granted user accounts or access to information systems or data. **Section 4.1.5 – IT Security Awareness, Training, and Education** – Updates entire section **Section 4.1.6 – Separation from Duty** – Updates policy element to require that all assets and data are recovered from departing individuals 4.1.6.b – Components shall establish procedures to ensure that all DHS information system-related property and assets are recovered from the departing individual and that sensitive information stored on any media is transferred to an authorized individual. Adds policy elements: 4.1.6.c - Accounts for personnel on extended absences shall be temporarily suspended. 4.1.6.d – System Owners shall review information system accounts supporting their programs at least annually. **Section 4.3.2 – Media Marking and Transport** – Adds "Transport" to section title and adds policy element: 4.3.2.b – Components shall control the transport of information system media containing sensitive data, outside of controlled areas and restrict the pickup, receipt, transfer, and delivery to authorized personnel. **Section 4.6 – Wireless Network Communications** – Updated section title from "Wireless Communication" and specifies "network communication" technologies in policy, rather than the more general "Wireless." Removes references to the defunct "WMO." **Section 4.6.1 – Wireless Systems** – Adds policy elements: 4.6.1.f – Component CISOs shall review all system applications for wireless usage, maintain an inventory of systems, and provide that inventory to the DHS CISO at least annually. 4.6.1.g – Component CISOs shall (i) establish usage restrictions and implementation guidance for wireless technologies; and (ii) authorize,

Version	Date	Description
		monitor, and control wireless access to DHS information systems. **4.9.1 – Security Incidents and Incident Response and Reporting** – Adds requirement for Components to maintain full SOC and CSIRC capability (May outsource to DHS SOC). Adds policy elements: 4.9.1.k – Components shall maintain a full SOC and CSIRC capability or outsource this capability to the DHS SOC. The DHS SOC shall provide SOC and CSIRC services to Components in accordance with formal agreements. Information regarding incident response capability is available in Attachment F of the DHS 4300A Sensitive Systems Handbook. 4.9.1.q – The DHS CISO shall publish Incident Response Testing and Exercise scenarios as required. 4.9.1.r – The Component CISO for each Component providing an incident response capability shall ensure Incident Response Testing and Exercises are conducted annually in coordination with the DHS CISO. **Section 5.1 – Identification and Authentication** – Adds requirement for strong authentication following HSPD-12 implementation. 5.1.f – Components shall implement strong authentication on servers, for system administrators and significant security personnel, within six (6) months of the Component's implementation of HSPD-12. **Section 5.4.1 – Remote Access and Dial-In** – Updates section and adds policy element: 5.4.1.f – The Public Switched Telephone Network (PSTN) shall not be connected to OneNet at any time. **5.4.3 – Network Connectivity** – Requires DHS CIO approval for all network connections outside of DHS. Also specifies requirement for CCB. 5.4.3.g – The DHS CIO shall approve all interconnections between DHS information systems and non-DHS information systems. Components shall document interconnections with an ISA for each connection. The DHS CIO shall ensure that connections with other Federal Government Agencies are properly documented. A single ISA may be used for multiple connections provided that the security accreditation is the same for all connections covered by that ISA. 5.4.3.l - The appropriate CCB shall ensure that documentation associated with an approved change to an information system is updated to reflect the appropriate baseline. DHS systems that interface with OneNet shall also be subject to the OneNet CCB. **Section 5.4.4 – Firewalls and Policy Enforcement Points** – Updates language to include Policy Enforcement Points. Adds policy elements: 5.4.4.i – The DHS CISO shall establish policy to block or allow traffic sources and destinations at the DHS TIC PEPs. The DHS CISO policy will prevent traffic as directed by the DHS CIO. 5.4.j – The DHS SOC shall oversee all enterprise PEPs. **Section 5.4.5 – Internet Security** – Prohibits Public Switched Telephone Network (PSTN) connection to OneNet.

Version	Date	Description
		5.4.5.a – Any direct connection of OneNet, DHS networks, or DHS mission systems to the Internet or to extranets shall occur through DHS Trusted Internet Connection (TIC) PEPSs. The PSTN shall not be connected to OneNet at any time. **Section 5.5.3 – Public Key/Private Key** – Assigns responsibility for non-human use of PKI to sponsors. 5.5.3.g – Sponsors for non-human subscribers (organization, application, code-signing, or device) shall be responsible for the security of and use of the subscriber's private keys. Every sponsor shall read, understand, and sign a "DHS PKI Subscriber Agreement for Sponsors" as a pre-condition for receiving certificates from a DHS CA for the non-human subscriber. **Section 5.4.6 – Email Security** – Prohibits auto-forwarding of DHS email to other than .gov or .mil addresses. 5.4.6.i - Auto-forwarding or redirecting of DHS email to address outside of the .gov or .mil domain is prohibited and shall not be used. Users may manually forward individual messages after determining that the risk or consequences are low. **Section 5.4.7 – Personal Email Accounts** – Requires use of encryption when sending sensitive information to email addresses other than .gov or .mil addresses. 5.4.7.b - When sending email to an address outside of the .gov or .mil domain, users shall ensure that any sensitive information, particularly privacy data, is attached as an encrypted file. **Section 5.6 – Malware Protection** – Updates term from "Virus."
7.1	September 30, 2009	**General Updates** Standardized the term "IT system" to "information system" Standardized the term "DHS IT system" to "DHS information system" Updated the term "DHS Security Operations Center" to "DHS Enterprise Operations Center" and added definition in glossary Replaced "must" with "shall" in all policy statements Replaced "vendors" with "others working on behalf of DHS" **Specific Updates** **Section 1.4.20** – Strong Authentication – Added definition for Strong Authentication **Section 1.4.21** – Two-Factor Authentication – Added definition for Two-Factor Authentication **Section 2.2.4** – Component Chief Information Officer – Alleviated confusion regarding Component CIO responsibilities **Section 2.2.5** – Chief Security Office – Removed erroneous CSO responsibilities which belong to Component CIOs **Section 2.2.7** – DHS Chief Financial Officer – Updated policy elements to clarify applicable policies

Version	Date	Description
		Section 3.1 – Basic Requirements (3.1.d, 3.1.g-j) – Updated policy elements to CISO/ISSM/ISSO responsibilities **Section 3.7.f** – Clarified Operating system exception requirements **Section 3.9.l-m** – Clarified requirements regarding TAF/RMS **Section 3.15** – CFO Designated Systems – Major revisions to this section **Section 4.6.2 and 5.4.1.a** – Prohibits tethering to DHS devices **Section 5.4.3.g-h** – Clarifies interconnection and ISA approval **Section 5.5** – Cryptography – Removed unnecessary elements from introductions and updated entire section with input from DHS PKI Steward
7.2	May 17, 2010	**General Updates** No general updates with this revision. Specific updates are listed below. **Specific Updates** **Section 1.4.8** – Added FISMA language (transmits, stores, or processes data or information) to definition of DHS System **Section 1.5.3.k** – Removed requirement for Component Head to make recommendation regarding waivers; removed requirement to report *exceptions* on FISMA report. **Section 2.1.6** – Adds requirement for AO to be a Federal employee **Section 2.1.7** – Clarifies that CO is a senior management official; stipulates that CO must be a Federal employee **Section 2.2.5** – Updated CSO role **Section 3.2** – Added intro to CPIC section and link to CPIC Guide **Section 3.5.2.h** – Added requirement to coordinate CP and COOP testing moderate and high FIPS categorizations **Section 3.15.a** – Added requirement for CFO Designated Systems security assessments for key controls be tracked in TAF and adds requirement for tracking ST&E and SAR annually. **Section 3.15.c** – Remaps control from RA-4 to RA-5 **Section 3.15.h** – Adds mapping to IR-6 **Section 3.15.i** – Remaps control from PL-3 to PL-2 **Section 3.17** – Added requirement to protect HIPAA information **Section 4.1.l.a** – Added requirement for annual reviews of position sensitivity levels **Section 4.1.1.c** – Exempts active duty USCG and other personnel subject to UCMJ from background check requirements **Section 4.1.4.c-d** – Adds additional separation of duties requirements and restricts the use of administrator accounts **Section 5.2.f** – Limits the number of concurrent connections for FIPS-199 high systems

Version	Date	Description
		Section 5.4.2.a – Limits network monitoring as per the Electronic Communications Act **Section 5.4.3** – Added introduction to clarify ISA requirements **Section 5.4.3.f** – Clarifies the term "security policy" in context **Section 5.4.3.m** – Clarifies that both AOs must accept risk for interconnected systems that do not require ISAs. **Section 5.4.3.m-n** – Adds stipulations to ISA requirements **Section 5.5** – Updates language in entire section **Section 5.5.3.j** – Assigns the DHS PKI MA responsibility for maintaining Human Subscriber agreements
7.2.1	August 9, 2010	**General Updates** No general updates with this revision. Specific updates are listed below. **Specific Updates** **Section 1.1** – Removes reference to 4300C **Section 1.4.1/3** – Updates Executive Order reference from 12958 to 13526 **Section 1.4.17** – Updates the PII section **Section 1.4.18** – Updates SPII section **Section 1.5.3** – Adds requirement for Privacy Officer/PPOC approval for exceptions and waivers pertaining to Privacy Designated Systems **Section 1.6.b/c** – Requires installation and use of digital signatures and certificates **Section 2.1.6.d** – Allows delegation of AO duty to review and approve administrators **Section 2.2.6** – Updates DHS Chief Privacy Officer description **Section 3.7.e** – Adds requirement to include DHS certificate as part of FDCC **Section 3.14** – Updates Privacy and Data Security section **Section 3.14.1** – Updates PII section **Section 3.14.2** – Updates PTA section **Section 3.14.2.e** – Updates impact level requirements for Privacy Sensitive Systems **Section 3.14.3** – Updates PIA section **Section 3.1.4.4** – Updates SORN section **Section 3.14.4.a** – Exempts SORN requirements **Section 3.14.5** – Updates Privacy Sensitive Systems protection requirements **Section 3.14.6.a** – Updates privacy incident reporting requirements

Version	Date	Description
		Section 3.14.7 – Updates privacy requirements for e-Auth **Section 3.14.7.e** – Adds PIA requirements for e-Auth **Section 4.1.1.e** – Expands U.S. citizenship requirement for access to all DHS systems and networks **Section 4.1.4.b** – Allows delegation of AO duty to review and approve administrators **Section 4.6.2.3.c** – Clarifies prohibited use of SMS **Section 4.8.4.h** – Updates the term "trusted" to "cleared" maintenance personnel **Section 4.12.i** – Updates escort requirements for maintenance or disposal **Section 4.12.j** – Requires disabling of dial up on multifunction devices **Section 5.4.3** – Clarifies definition of Network Connectivity **Section 5.4.3.m/n** – Clarifies requirement for ISA **Section 5.4.6.j** – Requires DHS email systems to use a common naming convention **Section 5.5.3.g** – Prohibits sharing of personal private keys
7.2.1.1	January 19, 2011	**General Updates** No general updates with this revision. Specific updates are listed below. **Specific Updates** **Section 4.8.1.a** – Changes requirement for screensaver activation from five (5) to fifteen (15) minutes of inactivity.
8.0	March 14, 2011	**General Updates** Update date and version number Replace "certification and accreditation" and "C&A" with "security authorization process". Replace "Certifying Official" with "Security Control Assessor". **Replace** "ST&E Plan" with "security control assessment plan". **Replace** "ST&E" with "security control assessment" **Replace** "system security plan" with "security plan" and "SSP" with "SP". **Specific Updates** **Section 1.4.8.1:** Change definition to specify that a GSS has only one ISSO. **Section 1.4.8.2:** Change definition to specify that an MA has only one ISSO. **Section 1.5.1:** Include language requiring waiver submissions to be coordinated with the AO. **Section 1.5.2:** Include language requiring waiver submissions to be coordinated with the AO. **Section 1.5.3:** Clarify language regarding submission of waivers and exceptions for CFO designated systems.

Version	Date	Description
		Section 1.6.d: Added new policy element, "DHS and Component systems shall be able to verify PIV credentials issued by other Federal agencies." **Section 2.1.2:** Add DHS CISO role as primary liaison to Component officials, and to perform periodic compliance reviews for selected systems. **Section 2.13:** Update Component CISO duties and add to implement POA&M process and ensure that eternal providers who operate information systems meet the same security requirements as the Component. **Section 2.1.4:** Update list of Component ISSM duties and create a POA&M for each known vulnerability. **Section 2.1.5:** Add significantly expanded Risk Executive duties. **Section 2.1.6:** Add significantly expanded Authorizing Official duties. **Section 2.2.8:** Add Program Manager responsibility for POA&M content. **Section 2.2.9:** Add expanded System Owner duties. **Section 2.2.11:** Renumber 2.2.10 as 2.2.11. **Section 2.2.10:** Add a new 2.2.10 to introduce and describe duties of Common Control Provider. **Section 3.2.g:** Added new policy element, "Procurements for services and products involving facility or system access control shall be in accordance with the DHS guidance regarding HSPD-12 implementation." **Section 3.5.2.c:** Updated language to clarify requirements for backup policy and procedures. **Section 3.5.2.f:** Updated language to require table-top exercises for testing the CP for moderate availability systems. **Section 3.7.f:** Added new policy element, "Components shall monitor USGCB (or DHS-approved USGCB variant) compliance using a NIST-validated Security Content Automation Protocol (SCAP) tool." **Section 3.9:** Add requirement for Components to designate a Common Control Provider. **Section 3.10.b:** Policy element language was updated to clarify the function of information system security review and assistance programs. **Section 3.14:** Language updated for readability. **Section 3.14.4.c:** Added new policy element, "Components shall review and republish SORNs every two (2) years as required by OMB A-130." **Section 3.14.7.f:** Added new policy element, "Existing physical and logical access control systems shall be upgraded to use PIV credentials, in accordance with NIST and DHS guidelines." **Section 3.14.7.g:** Added new policy element, "All new systems under development shall be enabled to use PIV credentials, in accordance with NIST and DHS guidelines, prior to being made operational." **Section 3.17:** Added reference to NIST SP 800-66 for more information on HIPAA. **Section 4.1.4.d:** Language updated to clarify usage of administrator accounts. **Section 4.1.5.f:** Language updated to clarify requirements for security

Version	Date	Description
		awareness training plan. **Section 4.3.1.b:** Language updated to clarify protection of offsite backup media. **Section 4.5.4:** Added reference to NIST SP 800-58 for more information on VoIP. **Section 4.9.j:** Language updated to require that Component SOCs report operationally to the respective Component CISO. **Section 4.9.k:** New policy element added, "The DHS EOC shall report operationally to the DHS CISO." **Section 4.10:** Revise list of annual system documentation updates. **Section 4.12.c:** Policy element replaced with new one stating that the policy applies "to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS data." **Section 5.4.1.e:** Policy element removed. **Section 5.4.1.f:** Policy element removed. **Appendix A:** Include new acronyms **Appendix B:** Revise definition of Accreditation Package to reflect new list of documentation. **Appendix C:** Update references
9.0	October 11, 2011	**General Updates** Various minor grammatical and punctuation changes were made throughout the document. Control references updated **Specific Updates** **Section 1.5.3.a:** New policy element added to state that the 4300A Policy and Handbook apply to all DHS systems unless a waiver or exception has been granted. **Section 2.1.3:** NPPD added to the list of Components having a fulltime CISO. **Section 2.1.8.g:** New policy element added to ensure ISSO responsibility for responding to ICCB change request packages. **Section 3.14.7.e:** Policy element revised to require consultation with a privacy officer to determine if a change requires an updated PTA. **Section 3.14.7.h:** New policy element added to ensure that all new DHS information systems or those undergoing major upgrades shall use or support DHS PIV credentials. **Section 4.1.5.d:** Policy element revised to clarify awareness training records requirements. **Section 4.1.5.e:** Policy element revised to clarify role-based training records requirements. **Section 4.1.5.g:** Policy element revised to require submission of an annual role-based training plan.

Version	Date	Description
		Section 4.1.5.j: Policy element revised to require annual DHS CISO review of role-based training programs. **Section 4.1.5.k:** Policy element revised to require biannual submission of roster of significant information security personnel and to specify the standard information security roles. **Section 4.3.1.f:** Policy element prohibiting connection of DHS removable media to non-DHS systems. It was already stated in 4.3.1.e. **Section 4.12.c:** Policy element was moved to 1.5.3.a. **Section 5.2.f:** Policy element revised to allow concurrent sessions to one if strong authentication is used. **Section 5.2.g:** New policy element added to ensure preservation of identification and access requirements for all data-at-rest.
9.0.1	March 5, 2012	**Section 2.1.3:** Includes 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. **Section 2.2.4:** Includes new language stating that the Component CISO reports directly to the Component CIO. **Section 4.1.1.c:** Includes new language to give Components the option to use background investigations completed by another Federal agency when granting system access to Federal employees. **Section 4.1.1.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.
9.0.2	March 19, 2012	**Throughout the document:** *EOC* and *Enterprise Operations Center* replaced with *SOC* and *Security Operations Center* respectively **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. **Section 1.8:** Section 1.8, Threats, was added to the policy. **Section 3.9.w:** Policy element added to require common control catalogs for DHS enterprise services. **Section 3.9.x:** Policy element added to require the development of Enterprise System Security Agreements for enterprise services. **Section 5.1.g:** Policy element added to require use of PIV credentials for logical authentication where available.
9.1	July 17, 2012	**General Changes** Style, grammar, and diction edited. Updated control references. Updated links. **Specific Changes** **Section 1:** Updated citations. **Section 1.6.b:** Changed to require use of electronic signatures where practicable.

Version	Date	Description
		Section 1.8.5: Section added defining *supply chain threat* and *supply chain.* **Section 2.1.3:** Added Science and Technology (S&T) to the list of Components that shall have fulltime CISOs. **Section 2.1.6.a:** Clarified language (designation of AOs at Department level). **Section 2.1.6.b:** Clarified language (designation of AOs at Component level). **Section 3.1.k:** Added policy statement requiring SCAP compliance. **Section 3.11.3:** Added section, including two policy statements, relative to Security Policy Working Group. **Section 3.14.6.e:** Updated reference title and hyperlink. **Section 3.18:** Section added containing Cloud Services policy. **Section 4.10:** Policy statements revised. **Section 4.1.1.c:** Changed "Minimum Background Investigation (MBI)" to "Moderate Risk Background Investigation (MBI)." **Section 4.1.5.k:** Changed "Contracting Officer Technical Representative" to "Contracting Officer Representative." **Section 4.3.1.d:** Changed policy statement to pertain only to USB drives. **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. **Sections and subsections 4.10 renumbered 4.91 and subsections** **Sections 4.11 through 4.13 renumbered 4.10 through 4.12** **Section 4.9.1.b:** Revised with clarification of reporting means and requirements. **Section 4.9.1.c:** Revised with clarification of reporting means and requirements. **Section 5.4.6.k:** Added policy statement moved from 5.4.7.b. **Section 5.4.7.b:** Deleted and becomes new policy statement 5.4.6.k. **Section 5.5.2** Section 5.5.2: Revised to address the two DHS PKIs now functioning: DHS FPKI and DHS Internal NPE PKI. **Section 5.5.3** Section 5.5.2: Revised to address the two DHS PKIs now functioning: DHS FPKI and DHS Internal NPE PKI. **Section 5.8:** Added new section, including two policy statements, relative to IT supply chain risks and protection against supply chain threats. **Appendix A, Acronyms and Abbreviations:** Additions and updates.
10.0	May 20, 2013	**General:** Changed version numbering system; all instances of "TAF" and "RMS" replaced with "IACS" throughout the document. **Section 1.5.3.n:** Included new policy element regarding expiration for exceptions. **Section 2.2.7.a:** Revised DHS CFO responsibility as AO for financial and mixed financial systems. **Section 3.11.4:** Included section on the ESSWG Section 3.18: Revised policy on cloud services/FedRAMP

Version	Date	Description
		Section 4.11: Revised policy on backup media protection. **Section 5.4.3:** Included new TIC traffic requirements.
11.0	April 30, 2014	**General:** Removed language regarding exceptions to policy from the document. **Section 1.5.2 and 4.1.1.e:** Revised to transfer responsibility to OCSO for granting access to IT systems by non-U.S. citizens. **Section 1.6:** Revised to align with NARA and OMB requirements and guidance on Electronic Signatures. **Section 3.18:** Revised policy on cloud services/FedRAMP **Section 4.62 (principally) and throughout:** "PED," "PDA," and "wireless PDA" have been replaced with the words "wireless mobile devices." **Section 5.5.2:** PKI policy element revisions throughout. Element 5.5.2.w, requiring appointment of Component PKI Managers, is rescinded. **Section 5.8:** Revised policy on supply chain
12.0	September 21, 2015	**General:** Updated FISMA references ("Federal Information Security Management Act " to "Federal Information Security Modernization Act of 2014"). **Section 1.4:** Alphabetized definition entries. **Section 1.4.7:** Removed statutory requirements language from FISMA definition **Section 1.4.14:** Revised definition of Personally Identifiable Information (PII) **Section 1.4.16:** Added definition of "privileged user" based on Cybersecurity Sprint communication **Section 1.4.19:** Revised definition of Sensitive Personally Identifiable Information. **Section 1.4.20:** Added definition of "Sensitive System" in response to Deputy CISO request **Section 1.4.21:** Revised definition of Strong Authentication based on Cybersecurity Sprint communication **Section 1.4.24:** Added definition of "visitor" in response to an OIG recommendation **Section 1.5.1.c:** Removed because the statement was procedure, not policy **Section 1.5.1.e:** Removed because the statement was procedure, not policy **Section 1.5.1.g:** Removed because the statement was procedure, not policy **Section 1.5.1.h:** Removed to align policy with actual procedure **Section 1.5.1.j:** Removed to align policy with actual procedure **Section 1.6:** Renamed to "Digital and Other Electronic Signatures"; section underwent major revision **Section 2.1.2:** Removed responsibilities related to COOP planning, security awareness training, and insider threat and Info Sec workforce development programs; added supply chain responsibilities **Section 2.1.3:** Removed responsibility related to execution of DHS Logging Strategy, which no longer exists **Section 2.1.4:** Added supply chain and software assurance responsibilities

Version	Date	Description
		Section 2.1.5: Added supply chain responsibilities **Section 2.1.7:** Security control assessor is assigned in writing by Component CISO or ISSM **Section 2.1.8:** Updated to require BIs for ISSOs; removed Secret clearance requirement **Section 2.2.3:** Added supply chain responsibilities **Section 2.2.4:** Added supply chain responsibilities **Section 2.2.8:** Added supply chain responsibilities and requirement to complete security control assessment for common controls **Section 2.2.9:** Added supply chain responsibilities **Section 3.7.i:** Added requirement for users to report IT changes to DHS Enterprise Configuration Management **Section 3.9.a:** Updated to include NIST SP 800-161 security controls in security authorization process **Section 3.9.b:** Updated to include NIST SP 800-161 security controls in security authorization process **Section 3.9.1:** Various changes throughout section **Section 3.14.1:** Per direction of the DHS Privacy Office, removed text following policy table **Section 3.14.1.g:** Removed; policy was incorporated into 3.14.1.f **Section 3.15.n:** Added supply chain responsibilities **Section 3.16:** Removed text following policy table **Section 4.1.4:** Replaced “separation of duties” with “segregation of duties” **Section 4.6.2.d:** Updated to include requirement for password complexity **Section 4.6.2.n:** Added to allow local access to mobile devices using fingerprint technology **Section 4.6.2.4:** Added new “Bluetooth” section **Section 4.8.4.d:** Revised to add requirement to protect against pass-the-hash & lateral movement vulnerabilities **Section 4.8.4.m:** Added requirement to include software assurance and supply chain in acquisition decisions **Section 4.8.4.n:** Added requirement to analyze COTS hardware and software for supply chain risk prior to procurement and upgrading **Section 5.1.c:** Updated to clarify policy related to disabling inactive user identifiers applies to all users **Section 5.1.g:** Revised based on Cybersecurity Sprint communication **Section 5.1.h:** Revised based on Cybersecurity Sprint communication **Section 5.1.k:** Added based on Cybersecurity Sprint communication **Section 5.1.l:** Added based on Cybersecurity Sprint communication **Section 5.3.j:** Added based on Cybersecurity Sprint communication **Section 5.4.2.a:** Updated continuous monitoring requirements to include information of third parties **Section 5.5.1.m:** Added to clarify PIV requirement **Section 5.5.1.n:** Added to clarify PIV requirement

Version	Date	Description
		Section 5.5.1.o: Added to clarify PIV requirement **Section 5.5.2:** Various changes throughout section **Section 5.5.3:** Various changes throughout section **Section 5.8.a:** Added to include NIST SP 800-161 security controls in security authorization process **Section 5.8.b:** Added to include NIST SP 800-161 security controls in security authorization process
12.01	February 12, 2016	**Section 1.6.2.c:** Updated to make the role of the signer mandatory in the visible signature block. **Section 5.4.6.l:** Added requirement for use of Government email accounts for Government business.