



# **DHS 4300A**

## **Sensitive Systems Handbook**

---

**INFORMATION TECHNOLOGY SECURITY PROGRAM**

Version 5.5

September 30, 2007

**DEPARTMENT OF HOMELAND SECURITY**

**DOCUMENT CHANGE HISTORY**

<b>Version</b>	<b>Date</b>	<b>Description</b>
1.0	January 13, 2003	Initial draft
1.1	January 24, 2003	Update
1.2	March 1, 2003	Content update, incorporation of review comments
1.3	June 20, 2003	Department policy
1.4	December 16, 2003	Content update, incorporation of review comments
2.0	March 31, 2004	Content update
2.1	July 26, 2004	Content update
3.0	April 30, 2005	Content update, including updates to PKI, Wireless Communications, Media Reuse, and Continuity Planning sections. Includes new sections on Required Reporting (FISMA) and Privacy Impact Assessments. New policies addressing use of C&A tool and DHS Hardening Guides. New attachments for IT Contingency Plan Template, Acronyms, and Media Reuse and Disposition.
3.1	July 29, 2005	New policy: 3.1b. Modified policies: 3.7c, 3.9g, 3.10a, 4.3.1.1b, 4.8.2.1a, 5.1.1.2b, 5.2.2a, 5.3c, 5.4.1.1a, 5.4.5.1d, 5.5.1.1a, 5.7d. Deleted policy in Section 5.4.8.1: policy requiring ISSMs to employ the automated DHS C&A tool for conducting vulnerability assessments was deleted because the tool does not do vulnerability assessments. Changes to password requirements in Section 5.1.1 and in Attachment L: change passwords every 180 days rather than every 90; don't use same password as last 8 passwords rather than last 6. New attachment: H (POA&M Process Guide). Revised attachments: C (ISSO Designation Letter), D (C&A Process), E (FISMA Reporting). Responsibility additions: added the Component CIO responsibility relating to DAA appointments. General: ITIM was replaced by CPIC; affected Sections 3.0, 3.2, 3.6.1; triple DES for encryption is no longer allowed, and references to FIPS 140-1 have been deleted.
3.2	October 1, 2005	Added Enclosure 1—DHS Secure Baseline Configuration Guides. Modified policies 3.8b, 4.8.1.1a, 5.2.1.1a&b, 5.2.2.1a, and 5.4.3.1c; combined (with modifications) policies 4.1e and 4.1f. Added Attachment J (Requesting Exceptions to Citizenship Requirement). Modified Sections 1.5, 3.13, 4.1, and 4.8.4.

Version	Date	Description
3.3	December 30, 2005	New policies: policies 3.9a–d; 3.11.1b; 4.6c; 5.4.3.1d&e. Modified policies: policies 3.9i&j; 4.3.1.1a; 4.3.2.1a; 4.6a, b; 4.6.1e; 4.6.2j; 4.6.2.1a; 4.6.3e; 5.4.3.1c; 5.5.2.1k. Revised sections: Sections 2.5; 2.7; 2.9; 2.11; 3.5.3.3 (references new Contingency Plan template); 3.9, 3.9.1 (type certification/accreditation); 3.9.1.1–3.9.1.5; 4.3; 4.3.1; 4.3.2; 4.6; 4.6.1–4.6.3; 5.4.3.1; 5.4.3.3; 5.5.2. Revised attachments: Attachment A (Requirements Traceability Matrix), Attachment K (new Contingency Plan template provided), Attachment N (ISAs).
4.0	June 1, 2006	New policies: 3.5.3.c&g, 4.6.2.3.c, 5.1.c, 5.2.c, 5.4.1.1.a. Modified policies: 3.5.1.c, 3.5.3.d–f, 3.7.a&b, 3.9.a&b, d, 4.1.4.1.b&c, 4.2.1.1.a, 4.3.1.1.a, 4.6.c, 4.6.1.a, 4.6.2.f, 4.10.3.1.a, 5.2.1.1.b, 5.3.a&b, 5.4.1.1.b, 5.4.3.1.a&c, 5.4.5.1.d. Certification and Accreditation section completely rewritten (Section 3.9). Expanded information on who serves as DAA (Section 2.9); reference to COOP Plan template removed (Section 3.5.1.3); modifications to Contingency Plan and Contingency Plan Test requirements (Sections 3.5.3, 3.5.3.1–3.5.3.5); “change management” changed to “configuration management” (Section 3.7); PIA responsibilities added (Section 3.14); modified information in Sections 4.6, 4.6.1, and 4.6.2; corrections to text in Section 5.4.3.1; change in “Signature and Comments” bullet in Section 5.4.3.2. New attachments: D (Type Accreditation), M (Tailoring the NIST SP 800-53 Security Controls). Modified attachments: A, E, F, G, H, I, K, L, N, O, U.
4.1	September 8, 2006	New policies: 3.14.1.a–c; 3.14.3.a–c; 4.10.1.1.c; 5.3.d&e; 5.4.1.1.c–e. Modified policies: 3.9.b; 4.6.2.d; 4.8.2.1.a–c; 4.10.1.1.b; 5.1.c; 5.3.c; 5.4.1.1.b. New sections: 3.14, 3.14.1, 3.14.3. Modified sections: 1.2, 2.9, 3.8.1.3, 3.9.1, 3.9.2, 4.8.2, 4.8.2.1, 4.8.2.2, 4.10.1, 4.10.1.1; 4.10.1.2, 5.1.4.4, 5.2.3.1, 5.2.3.2.
4.2	September 29, 2006	New policies: 4.6.4.a–f. Modified policies: 4.3.3.1.a–c. Rewritten section: 4.3.3. New section: 4.6.4.
5.0	March 1, 2007	New policies: 4.1.5.h. Modified policies: 3.10.c, 4.1.1.d, 4.1.5.a,b,f,&g, 4.6.2.d, 4.6.3.f, 5.2.c, 5.4.8.a, 5.6.b. New sections: 4.1.1. Modified sections: 1.2, 1.4.2, 1.4.3, 2.9, 3.2, 3.4, 3.5.2, 3.5.3, 3.9, 3.9.1, 3.9.11, 3.10, 3.10.3, 3.12, 3.13, 4.1.1, 4.1.5, 4.1.5.2, 4.3.2, 4.6.1, 4.6.2, 4.6.3, 4.6.4, 4.8.5, 4.9, 4.12, 5.1.1, 5.1.1.1, 5.2, 5.2.1, 5.2.2, 5.2.3. Renumbered sections: 4.1.2–4.1.6, 4.9, 4.10, 4.11, 4.12. New attachments: Q1, Q2, Q3, Q4.

Version	Date	Description
		Updated attachments: A, F, G, H.
5.1	April 18, 2007	Update based on SOC CONOPS, Final Version 1.4.1, April 6, 2007; Adds DHS Chief Financial Officer – Designated Financial Systems; Updates the term, <i>Sensitive But Unclassified</i> to <i>For Official Use Only</i>
5.2	June 1, 2007	Updates Sections 2.7, 2.9, 2.12, 3.3, 3.5.1, 3.5.3, 3.6, 3.8, 3.9, 3.10, 3.14, 3.15, 4.1.5, 4.1.6, 4.10, 4.12, 5.1.1, 5.2, 5.3, 5.4.1, 5.4.3, 5.4.4, 5.4.8, 5.5.1, 5.7
5.3	August 3, 2007	Revised policy in Sections 3.5.1 and 5.5.1, and removed Section 3.5.2. Removed Sections 3.11.2 and 3.11.4
5.4	September 30, 2007	Content update, incorporation of change requests
5.5	September 30, 2007	<p><b>List of Attachments</b> Addition of Attachment R, Compliance Framework for CFO designated Financial Systems, to list of attachments.</p> <p><b>Section 1.0:</b> 1.1 – Added text regarding policy implementation and DHS security compliance tool updates. 1.2 – Inserted full title of “Ethical conduct for Employees for the Executive Branch”; removed two other references; deleted "various" from citation of standards. 1.4.13 - Added definition for operational data.</p> <p><b>Section 2.0:</b> 2.0 – Insert the following after the first sentence in the second paragraph: “Security is an inherently governmental responsibility. Contractors and other sources may assist in the performance of security functions, but a government individual must always be designated as the responsible agent for all security requirements and functions.” 2.3 – Removed parentheses from "in writing."</p> <p><b>Section 3.0:</b> 3.9 – Deleted title above policy table. 3.9 – Inserted new policy element “l” regarding CISO concurrence for accreditation. 3.9j – Updated NIST SP 800-53 Security Controls table. 3.15 – Added text regarding Component CFOs and ISSMs.</p>

Version	Date	Description
		<p><b>Section 4.0:</b> 4.1.1 – Capitalized “Background,” and added "(BI).” 4.3.1 – Two new elements were added to the policy table. 4.7 – Inserted "where required or appropriate" before the sentence. 4.8.3 – Title changed to “Personally Owned Equipment and Software (not owned by or contracted for by the Government).” 4.8.6 – Included new section regarding wireless settings for peripheral equipment.</p> <p><b>Section 5.0:</b> 5.1c – Changed inactive accounts to “disable user identifiers after 45 days of inactivity.” 5.1.1 – First sentence of the second paragraph was rewritten to prohibit use of personal passwords by multiple individuals. 5.2.2 – Title changed to “Automatic Session Termination.” 5.4.8 – Added text regarding clearance level for vulnerability scanning.</p> <p><b>Attachment M:</b> Updated Excel spreadsheet, M – 800-53 Controls, to include control enhancements. Updated date and version number to coincide with current Handbook.</p>

## TABLE OF CONTENTS

<b>1.0</b>	<b>INTRODUCTION.....</b>	<b>1</b>
1.1	IT Security Program Policy and Implementation Guidelines.....	1
1.2	Authorities .....	2
1.3	Policy Overview .....	3
1.4	Definitions .....	3
1.4.1	Classified National Security Information .....	3
1.4.2	National Intelligence Information.....	3
1.4.3	Sensitive Information.....	3
1.4.4	Public Information .....	4
1.4.5	Information Technology (IT).....	4
1.4.6	DHS IT System.....	4
1.4.6.1	General Support System (GSS).....	4
1.4.6.2	Major Application (MA) .....	5
1.4.7	Component.....	5
1.4.8	Trust Domain .....	5
1.4.9	Continuity of Operations .....	5
1.4.10	Continuity of Operations Plan .....	5
1.4.11	Essential Functions .....	5
1.4.12	Vital Records .....	5
1.4.13	Operational Data.....	6
1.5	Waivers and Exceptions.....	6
1.6	Information Sharing Strategy.....	6
1.7	Threats .....	7
1.7.1	Internal Threats .....	8
1.7.2	Criminal Threats .....	8
1.7.3	Foreign Threats .....	8
<b>2.0</b>	<b>ROLES AND RESPONSIBILITIES.....</b>	<b>10</b>
2.1	Secretary of Homeland Security .....	10
2.2	Under Secretaries and Heads of DHS Components.....	10
2.3	DHS Chief Information Officer (CIO) .....	11
2.4	Component Chief Information Officers.....	11
2.5	Chief Information Security Officer (CISO).....	12
2.6	Office of the Chief Privacy Officer (CPO).....	13
2.7	DHS Chief Security Officer (CSO) .....	13
2.8	Component Information Systems Security Manager (ISSM).....	13
2.9	Component Privacy Offices and Privacy Points of Contact (PPOC) .....	14
2.10	Program Manager (PM).....	15
2.11	United States Computer Emergency Readiness Team (US-CERT) .....	15
2.12	Certifying Official.....	16
2.13	Designated Accrediting Authority (DAA).....	16
2.14	Information Systems Security Officer (ISSO).....	17
2.15	System Owners .....	17

2.16	Users of Supplied Computing Resources .....	18
2.17	Additional Personnel.....	18
2.18	DHS Chief Financial Officer designated Financial Systems.....	18
2.18.1	DHS CFO.....	18
2.18.2	DHS CIO.....	19
2.18.3	Component CFO .....	20
2.18.4	Component CIO .....	20
2.18.5	System Owners .....	21
<b>3.0</b>	<b>MANAGEMENT CONTROLS.....</b>	<b>22</b>
3.1	Basic Requirements .....	22
3.2	Capital Planning and Investment Control.....	23
3.3	Contractors and Outsourced Operations .....	25
3.4	Performance Measures and Metrics.....	27
3.5	Continuity Planning for Critical DHS Assets .....	28
3.5.1	Continuity of Operations Planning .....	28
3.5.1.1	COOP Planning Requirement.....	30
3.5.1.2	COOP Planning Objectives .....	30
3.5.1.3	COOP Plan Content.....	30
3.5.1.4	COOP Test, Training, and Exercise (TT&E).....	31
3.5.2	IT Contingency Planning .....	31
3.5.2.1	IT Contingency Planning Requirement .....	33
3.5.2.2	IT Contingency Plan Development .....	34
3.5.2.3	IT Contingency Plan Format and Content.....	34
3.5.2.4	IT Contingency Plan Test and Exercise .....	34
3.5.2.5	IT Contingency Plan Training .....	34
3.6	System Development Life Cycle .....	35
3.6.1	Planning .....	36
3.6.2	Requirements Definition.....	37
3.6.3	Design .....	37
3.6.4	Development.....	37
3.6.5	Test.....	38
3.6.6	Implementation .....	38
3.6.7	Operations and Maintenance .....	38
3.6.8	Disposition .....	38
3.7	Configuration Management .....	39
3.8	Risk Management .....	41
3.8.1	Risk Assessment .....	43
3.8.2	Risk Mitigation .....	43
3.8.3	Evaluation and Assessment .....	44
3.9	Certification and Accreditation, Remediation, and Reporting .....	44
3.9.1	FIPS 199 Categorization and the NIST SP 800-53 Controls.....	49
3.9.2	Privacy Impact Assessment (PIA) .....	60
3.9.3	E-Authentication.....	61
3.9.4	Risk Assessment .....	61
3.9.5	System Security Plan (SSP).....	61

3.9.6	Contingency Plan .....	62
3.9.7	Security Test and Evaluation (ST&E) Plan .....	62
3.9.8	Contingency Plan Testing .....	63
3.9.8.1	Systems with High Impact Availability — <i>Testing required</i> .....	63
3.9.8.2	Systems with Moderate Impact for Availability — <i>Testing required</i> .....	64
3.9.8.3	Systems with Low Impact for Availability — <i>Testing optional</i> .....	64
3.9.9	Security Assessment Report (SAR) .....	64
3.9.10	Authorization to Operate (ATO) Letter .....	65
3.9.11	Annual Self-Assessments .....	66
3.10	IT Security Review and Assistance .....	67
3.10.1	Review and Assistance Management and Oversight .....	68
3.10.2	IT Security Assistance .....	68
3.10.3	IT Security Reviews .....	69
3.11	Security Working Groups and Forums .....	69
3.11.1	DHS Information Systems Security Board .....	69
3.11.2	DHS IT Security Training Working Group .....	69
3.11.3	DHS Wireless Security Working Group (WSWG) .....	70
3.12	IT Security Policy Violation and Disciplinary Action .....	70
3.13	Required Reporting .....	71
3.14	Privacy and Data Security .....	72
3.14.1	Personally Identifiable Information .....	72
3.14.2	Privacy Impact Assessments .....	73
3.14.3	Privacy Incident Reporting .....	74
3.14.4	E-Authentication .....	75
3.15	DHS Chief Financial Officer – Designated Financial Systems .....	75
<b>4.0</b>	<b>OPERATIONAL CONTROLS .....</b>	<b>79</b>
4.1	Personnel .....	79
4.1.1	Citizenship, Personnel Screening, and Position Categorization .....	79
4.1.1.1	Background Investigations for Government Employees .....	80
4.1.1.2	Background Investigations for Contractor Personnel .....	81
4.1.2	Rules of Behavior .....	82
4.1.3	Access to Sensitive Information .....	83
4.1.4	Separation of Duties .....	84
4.1.5	IT Security Awareness, Training, and Education .....	85
4.1.5.1	Initial Awareness .....	88
4.1.5.2	Refresher Awareness .....	89
4.1.5.3	Ongoing Awareness Activities .....	89
4.1.5.4	Role-Based Training .....	89
4.1.6	Separation from Duty .....	89
4.2	IT Physical Security .....	91
4.2.1	General Physical Access .....	92
4.2.1.1	Physical Controls .....	93
4.2.1.2	Building Passes .....	94
4.2.1.3	Property Removal .....	94

	4.2.1.4	Loss or Theft of Property .....	94
	4.2.1.5	Environmental Controls.....	94
	4.2.1.6	Fire Protection .....	95
	4.2.1.7	Electronic Power Supply Protection.....	95
	4.2.1.8	Temperature and Humidity Control .....	95
	4.2.1.9	Housekeeping Considerations .....	96
	4.2.1.10	Personnel Safety Features.....	96
	4.2.1.11	Emergency Exits.....	96
	4.2.2	Sensitive Facility.....	96
4.3		Media Controls .....	97
	4.3.1	Media Protection.....	97
	4.3.2	Media Marking .....	98
	4.3.3	Media Sanitization and Disposal .....	100
	4.3.4	Production, Input/Output Controls .....	103
4.4		Voice Communications Security .....	104
	4.4.1	Private Branch Exchange.....	104
	4.4.1.1	Maintenance Vulnerabilities.....	107
	4.4.1.2	Software Loading and Update Tampering .....	108
	4.4.1.3	User Features .....	108
	4.4.2	Telephone Communications .....	109
	4.4.3	Voice Mail .....	110
4.5		Data Communications.....	111
	4.5.1	Telecommunications Protection Techniques .....	111
	4.5.2	Facsimiles .....	112
	4.5.3	Video Teleconferencing.....	114
	4.5.4	Voice over Data Networks.....	115
4.6		Wireless Communications .....	117
	4.6.1	Wireless Systems .....	119
	4.6.2	Wireless Portable Electronic Devices.....	121
	4.6.2.1	Cellular Phones.....	124
	4.6.2.2	Pagers .....	125
	4.6.2.3	Multifunctional Wireless Devices .....	126
	4.6.3	Wireless Tactical Systems .....	127
	4.6.4	Radio Frequency Identification (RFID).....	129
4.7		Overseas Communications.....	130
4.8		Equipment .....	131
	4.8.1	Workstations .....	132
	4.8.2	Laptop Computers and Other Mobile Computing Devices .....	133
	4.8.3	Personally Owned Equipment and Software (Not owned by or contracted for by the Government).....	135
	4.8.4	Hardware and Software.....	136
	4.8.5	Personal Use of Government Office Equipment and DHS IT Systems/Computers.....	138
	4.8.6	Wireless Settings for Peripheral Equipment.....	140
4.9		Security Incidents and Incident Response and Reporting .....	141
	4.9.1	Law Enforcement Incident Response .....	143

4.9.2	Definitions and Incident Categories .....	144
4.9.3	DHS Security Operations Center .....	145
4.10	Documentation (Manuals, Network Diagrams).....	145
4.11	Information and Data Backup.....	147
4.12	Converging Technologies .....	150
<b>5.0</b>	<b>TECHNICAL CONTROLS.....</b>	<b>152</b>
5.1	Identification and Authentication .....	152
5.1.1	Passwords.....	153
5.1.1.1	Selecting Strong Passwords.....	154
5.1.1.2	Results of Weak Passwords.....	155
5.1.1.3	System Administrator Responsibilities .....	156
5.2	Access Control.....	157
5.2.1	Automatic Account Lockout.....	159
5.2.2	Automatic Session Termination.....	160
5.2.3	Warning Banner .....	160
5.3	Auditing .....	162
5.4	Network and Communications Security .....	164
5.4.1	Remote Access and Dial-In .....	164
5.4.2	Network Security Monitoring.....	166
5.4.2.1	What Is Intrusion Detection?.....	167
5.4.2.2	Methods and Techniques.....	167
5.4.2.3	Monitoring.....	167
5.4.3	Network Connectivity.....	168
5.4.3.1	Interconnection Security Agreements .....	169
5.4.4	Firewalls.....	170
5.4.4.1	Firewall Basics .....	171
5.4.4.2	Firewall Deployment .....	172
5.4.5	Internet Security.....	172
5.4.6	Email Security.....	175
5.4.7	Personal Email Accounts .....	178
5.4.8	Testing and Vulnerability Management .....	180
5.4.8.1	Scope of Vulnerability Assessments .....	183
5.4.9	Peer-to-Peer Technology .....	183
5.5	Cryptography .....	185
5.5.1	Encryption.....	186
5.5.2	Public Key Infrastructure.....	187
5.5.3	Public Key/Private Key .....	190
5.6	Virus Protection .....	193
5.6.1	What Is a Virus? .....	195
5.6.2	Other Types of Malicious Code.....	195
5.6.3	How Viruses and Other Malicious Code Affect Systems.....	196
5.6.4	Procedures When a Virus Is Detected on a System.....	196
5.7	Product Assurance .....	196
<b>6.0</b>	<b>DOCUMENT CHANGE REQUESTS.....</b>	<b>199</b>
<b>7.0</b>	<b>QUESTIONS AND COMMENTS.....</b>	<b>199</b>

**Enclosure 1—DHS Secure Baseline Configuration Guides (February 28, 2007)**

- Cisco Router Secure Baseline Configuration Guide
- HP-UX Secure Baseline Configuration Guide
- Linux Secure Baseline Configuration Guide
- Solaris Secure Baseline Configuration Guide
- Solaris 10 Secure Baseline Configuration Guide
- Windows Secure Baseline Configuration Guide
- SQL Server Secure Baseline Configuration Guide
- ORACLE Secure Baseline Configuration Guide
- Legacy Windows NT Configuration Guidance
  - Guidance for Securing Windows NT
  - Level One Benchmark Windows NT 4-0 Operating Systems V1.0.5
  - Guide to Securing Microsoft Windows NT Network
  - Addendum to the NSA Guide to Securing Microsoft Windows NT Networks and NSA Guides to Securing Windows 2000
- Windows 2003 Server/Windows XP/Windows Vista Secure Baseline Configuration Guide

**Attachment A—Requirements Traceability Matrix****Attachment B—Waivers and Exceptions Request Form****Attachment C—Information Systems Security Officer Designation Letter****Attachment D—Type Accreditation****Attachment E—FISMA Reporting****Attachment F—Incident Response and Reporting****Attachment G—Rules of Behavior****Attachment H—Plan of Action and Milestones (POA&M) Process Guide****Attachment I—Workstation Logon, Logoff, and Locking Procedures****Attachment J—Requesting Exceptions to Citizenship Requirement****Attachment K—IT Contingency Plan Template****Attachment L—Password Management****Attachment M—Tailoring the NIST SP 800-53 Security Controls****Attachment N—Preparation of Interconnection Security Agreements**

**Attachment O—Vulnerability Assessment Program**

**Attachment P—Document Change Requests**

**Attachment Q1—Wireless Systems**

**Attachment Q2—Wireless Portable Electronic Devices**

**Attachment Q3—Wireless Tactical Systems**

**Attachment Q4—Sensitive RFID Systems**

**Attachment S—Unassigned**

**Attachment R—Compliance Framework for CFO Designated Financial Systems**

**Attachment T—Acronyms and Abbreviations**

## **1.0 INTRODUCTION**

This handbook serves as a foundation for Components within the Department of Homeland Security (DHS) to develop and implement their information technology (IT) security programs. The purpose of this document is to provide specific techniques and procedures for implementing the requirements of the DHS IT Security Program for Sensitive Systems. These baseline security requirements (BLSRs) are generated by the DHS IT security policies published in DHS Sensitive Systems Policy Directive 4300A. The BLSRs included in this handbook (see Attachment A, Requirements Traceability Matrix) must be addressed in the IT security documents prepared by each Component.

This handbook incorporates many of the procedures in use by security personnel from the various organizations from which the DHS was formed. Therefore, it is a compilation of the best practices used by DHS Components. In addition, it implements as requirements many of the guidelines contained in various National Institute of Standards and Technology (NIST) publications, Office of Management and Budget (OMB) direction, and Congressional as well as Executive Branch mandates.

The scope and contents of this handbook will change over time as new capabilities are added to DHS systems, as security standards are upgraded, and as a result of user experience and comment. As the DHS IT Security Program matures, individual attachments to the handbook addressing specific security areas of interest, such as password management, contingency planning, and certification and accreditation, will be developed and published. Several have already been developed and are included as attachments to this handbook.

This handbook is issued as implementation guidance under the authority of the Chief Information Officer through the Office of the Chief Information Security Officer. As such, it supersedes directives of the Departments to which the Components formerly reported. This handbook addresses IT security only. Documents addressing personnel, physical, information, and industrial security; investigations; emergency preparedness; and domestic counterterrorism will be issued separately by the agencies responsible for these programs. However, those aspects of personnel, physical, information and industrial security; investigations; emergency preparedness; and counterterrorism that relate to IT security are addressed in this handbook.

See Section 7.0 for information on requesting clarification of DHS IT security policies and procedures.

### **1.1 IT Security Program Policy and Implementation Guidelines**

The DHS IT Security Program provides a set of BLSRs for use by DHS Components. This handbook provides procedures and techniques necessary to implement those BLSRs relating to management, operational, and technical controls that provide the foundation necessary to ensure confidentiality, integrity, availability, authenticity, and nonrepudiation within the DHS IT infrastructure and operations.

This handbook addresses the procedures necessary for implementing security requirements for sensitive IT systems. DHS policy mandates that all DHS computing resources be individually accounted for as part of an IT system. IT systems encompass major applications and general support systems.

The DHS IT Security Program does not apply to any IT that processes, stores, or transmits foreign intelligence information pursuant to Executive Order (E.O.) 12333, to Director of Central Intelligence directives governing the protection of intelligence information, and to other applicable orders.

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

## 1.2 Authorities

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

- Federal Information Security Management Act (FISMA) of 2002, November 25, 2002
- Federal Financial Management Improvement Act of 1996 (FFMIA), P.L. 104-208
- Federal Managers' Financial Integrity Act of 1982 (FMFIA), P.L. 97-255
- The National Security Act of 1947, dated July 26, 1947
- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987
- Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996
- Public Law 107-296, Homeland Security Act of 2002
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch
- Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, dated April 3, 1984
- Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities*, dated November 18, 1988, as amended
- Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*
- OMB Circular A123, *Management's Responsibility for Internal Control*, Revised, December 21, 2004
- OMB Circular A-127, *Financial Management Systems*, Revised December 1, 2004
- OMB Bulletin 06-03, *Audit Requirements for Federal Financial Statements* August 23, 2006
- Department of Homeland Security Acquisition Regulation (HSAR), June 2006

- DHS Management Directives (e.g., MD 0470.1, MD 1030, MD 4400.1, MD 4500.1, MD 4600.1, MD 11042.1, MD 11050.2)
- National Institute of Standards and Technology (NIST) Special Publications (e.g., 800-16, 800-34, 800-37, 800-50, 800-53 Revision 1) and Federal Information Processing Standards (FIPS) (e.g., FIPS 199, 200)
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000

### 1.3 Policy Overview

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

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

### 1.4 Definitions

The following definitions apply to the policies and procedures outlined in this document. Other definitions may be found in the National InfoSec Glossary ([http://www.cnss.gov/Assets/pdf/cnssi\\_4009.pdf](http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf)).

#### 1.4.1 Classified National Security Information

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

#### 1.4.2 National Intelligence Information

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

#### 1.4.3 Sensitive Information

“Sensitive information” is information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security Number; trade

secrets; system vulnerability information; pre-solicitation procurement documents, such as statements of work; and law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies in internal controls are also sensitive information because of the potential damage that could be caused by the misuse of this information. This type of information concerning financial systems will be identified as Sensitive Financial Information, if on another system it would be identified as system vulnerability information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access.

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

#### **1.4.4 Public Information**

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

#### **1.4.5 Information Technology (IT)**

The Clinger-Cohen Act defines information technology as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an Executive agency.

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

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

#### **1.4.6 DHS IT System**

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

##### **1.4.6.1 General Support System (GSS)**

A general support system (GSS) is an interconnected set of information resources under the same direct management control that share common functionality. A GSS normally includes hardware, software, applications, data and users. Examples of a GSS include a local area network (LAN), an agencywide backbone, a communications network, a data processing center, a tactical radio network, or a shared information processing service organization.

### **1.4.6.2 Major Application (MA)**

A major application (MA) is an automated information system (AIS) that “requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.<sup>1</sup>” An MA is distinguishable from a GSS by the fact that it is a discrete application, whereas a GSS may support multiple applications.

### **1.4.7 Component**

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

### **1.4.8 Trust Domain**

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

### **1.4.9 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 IT systems; specify succession to office and the emergency delegation of authority; provide for the safekeeping of vital records and databases; identify alternate operating facilities; provide for interoperable communications; and validate the capability through tests, training, and exercises.

### **1.4.10 Continuity of Operations Plan**

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

### **1.4.11 Essential Functions**

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

### **1.4.12 Vital Records**

Electronic and hardcopy documents, references, records, databases, and IT systems needed to support essential functions under the full spectrum of emergencies. Categories of these types of records may include:

---

<sup>1</sup> OMB Circular A-130

- *Emergency operating records*—emergency plans and directive(s), orders of succession, delegations of authority, staffing assignments, selected program records needed to continue the most critical agency operations, as well as related policy or procedural records.
- *Legal and financial rights records*—protect the legal and financial rights of the Government and of the individuals directly affected by its activities. Examples include accounts receivable records, social security records, payroll records, retirement records, and insurance records. These records were formerly defined as “rights-and-interests” records.
- *Records used to perform national security preparedness functions and activities (E.O. 12656).*

### **1.4.13 Operational Data**

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

## **1.5 Waivers and Exceptions**

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

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

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

NOTE: Special procedures apply for exception to the requirement that persons accessing DHS systems be U.S. Citizens (policy 4.1e). Under normal conditions, only U.S. Citizens are allowed access to DHS systems and networks, however, at times there is a need to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to appropriate policies are treated separately from standard exceptions and waivers. The approval chain for an exception to the U.S. Citizenship requirement flows through the Component Head, the Office of Security, and the Chief Information Officer. Attachment J to the DHS 4300A Sensitive Systems Handbook provides an electronic form for requesting exceptions to the U.S. Citizenship requirement.

## **1.6 Information Sharing Strategy**

The DHS SOC exchanges information with Component SOCs, NOCs, the HSDN SOC, the Intelligence Community, and with external organizations in order to facilitate the security and operation of the DHS network. This exchange enhances situational awareness and provides a common operating picture to network managers. The operating picture is developed from

information obtained from “raw” fault, configuration management, accounting, performance, and security data. This data is monitored, collected, analyzed, processed, and reported by the NOCs and SOCs.

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

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

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

## **1.7 Threats**

We live in a highly interconnected world where computers rarely function in a single enclave. Computers are typically connected to the Internet, to all parts of an organization, and to other organizations, both public and private. There is also an increased emphasis within the Federal Government on telecommuting, which requires remote connections to a network, either through dial-in, cable, or digital subscriber line (DSL) connections. In addition, building management services (e.g., badge systems; heating, ventilating, and air-conditioning (HVAC); and entry) may also be connected to the network.

Wireless systems permit personnel to be in touch with their office, whether by cell phone, pager, or other portable electronic device. Wireless local area networks (WLAN) permit personnel to connect to their network at various locations throughout a building, contingent upon adequate signal coverage.

Technologies are also converging. Cell phones now can also be used for Internet and email access, for “walkie-talkie” like communications, and even for video. Voice over Internet Protocol (VoIP) permits cost savings by combining voice and data services into one network. Copiers now also perform network printing, permit printing over the Internet, and provide facsimile (fax) functions.

The increased emphasis on e-Government has provided a new class of Government computer user—namely, the general public. Emphasis on a paperless office is moving the sole repository for official records from paper to electronic media.

Each of these technology advancements contain inherent security risks and as such present challenges to DHS security professionals in countering these added threats. The following paragraphs discuss internal, criminal, and foreign threats to DHS systems.

### **1.7.1 Internal Threats**

Managers are aware of the usual natural and physical threats to computer systems, such as earthquakes, tornadoes, fires, floods, electric outages, and plumbing disasters, but may not have the same level of awareness with respect to manmade disasters and threats. Employees tend to be computer literate; most have computers at home. In light of that literacy, the threat from Departmental employees and/or contractors should not be underestimated. A malicious authorized user can damage to DHS's reputation and to its data. A careless user can inflict similar damage. Sensitive data, some official records, can be lost, corrupted, or compromised through malicious or careless acts. Email can be used, either deliberately or without thought, to transmit sensitive data outside the Department to recipients or other computer systems that are not authorized to receive or store the data. A malicious authorized user may also use Departmental computers to attack other computers within and outside of DHS.

Converging technologies combine the vulnerabilities of each technology and add new ones. Care must be taken to ensure systems are designed with no single points of failure. For example, if the Department were using VoIP, it would want to ensure that an outage on its data network would not also cause an outage on its voice network (telephone and fax). Similarly, if the building HVAC were connected to the data network, the Department would want to ensure that an outage or attack on its data network would not also create an outage on the HVAC (and vice versa).

### **1.7.2 Criminal Threats**

Malicious code of all varieties remains a threat to our computer systems. Virus writing tools are available that enable even inexperienced persons to write viruses, and malicious software is becoming much more sophisticated. Email software provides capabilities such as scripting, which allows power users to create email messages that can be tailored to the recipient. These capabilities may also be used to destroy data on computers and to export malicious code to everyone in the organization's address book. Malicious code can also place backdoors into the network that would permit access to data or resources on the network.

The hacker community now provides scripts so that even the neophyte can exploit network vulnerabilities. Exploits for vulnerabilities in software are often published on the hacker sites days after the vulnerability is published. Skilled hackers are targeting e-commerce sites to obtain credit card numbers, which they then sell. Persons with hacking skills are hired by organizations to perform industrial espionage. All they need to do is read or copy a file. They can be in and out of a network without leaving a trace.

Theft of equipment, particularly laptops, is also increasing. Data on a laptop, if not encrypted, can reveal critical information, such as changes to legislation, investigations, or economic analyses. Thefts occur regularly from offices, airports, automobiles, and hotel rooms.

### **1.7.3 Foreign Threats**

Foreign Governments conduct espionage to protect themselves against perceived threats from the United States as well as to obtain information that will be useful to their own industrial base. Terrorists may now have the skills to disrupt Internet communications. Hacker groups have launched successful attacks against networks of countries they oppose.

Wireless communications are easy to eavesdrop. The equipment for doing so is commercially available. “War driving” to detect wireless access points is the latest technique used by hackers and spies to obtain access to wireless networks. Employees overseas should assume their cell phone conversations are being monitored.

Many software manufacturers outsource software code development, some of it offshore to foreign countries. Any outsourcing operation raises concerns about the quality of the product produced and invites speculation about whether malicious or criminal code has been inserted in the software. Indeed, it is becoming increasingly difficult to determine the actual source of an organization’s IT because code and equipment are assembled from so many sources.

## **2.0 ROLES AND RESPONSIBILITIES**

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

Designated personnel play a major role in the planning and implementation of IT security requirements. Security is an inherently governmental responsibility. Contractors and other sources may assist in the performance of security functions, but a government individual must always be designated as the responsible agent for all security requirements and functions. The following presents a list of roles and responsibilities for implementing these requirements.

Additional responsibilities for each of the roles are provided in Section 3.0 (Management Controls), Section 4.0 (Operational Controls), and Section 5.0 (Technical Controls).

### **2.1 Secretary of Homeland Security**

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

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

### **2.2 Under Secretaries and Heads of DHS Components**

The Under Secretaries and the heads of DHS Components:

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

### **2.3 DHS Chief Information Officer (CIO)**

The DHS Chief Information Officer (CIO) will establish and oversee the Department-wide IT Security Program, ensure proper computer security incident response, and provide consulting assistance to all DHS offices for their individual programs. The DHS CIO provides management direction for the DHS Security Operations Center (SOC) and overall direction for Component SOCs. The DHS CIO, or designated representative, has the sole responsibility for public release of information concerning computer security incidents. The CIO will consult with the DHS Privacy Office and Public Affairs Office prior to releasing any information.

The DHS CIO:

- Appoints a Federal employee in writing to serve as the DHS Chief Information Security Officer (CISO).
- Serves as the Designated Accrediting Authority (DAA) for DHS enterprise IT systems. This responsibility may be delegated in writing as appropriate.
- Participates in developing DHS performance plans, including descriptions of the time periods and budget, staffing, and training resources required to implement the Department-wide security program.
- Ensures that all IT systems acquisition documents, including existing contracts, include appropriate IT security requirements and comply with DHS IT security policies.
- Ensures that DHS security programs integrate fully into the DHS enterprise architecture and capital planning and investment control processes.
- Ensures that system owners understand and appropriately address risks, including interconnectivity with other programs and systems outside their control.
- Reviews and evaluates the IT Security Program annually.
- Ensures that an IT security performance metrics program is developed, implemented, and funded.
- Reports to the Under Secretary for Management on matters relating to the security of DHS IT systems.

### **2.4 Component Chief Information Officers**

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

Component Chief Information Officers (CIO):

- Establish and oversee their Component IT security programs.
- Ensure that a Component Information System Security Manager (ISSM) has been appointed.
- Ensure that a Designated Accrediting Authority (DAA) has been appointed for all Component IT systems and serve as the DAA for any IT system where a DAA has not been appointed or where a vacancy exists.

- Ensure that IT security concerns are addressed by Component Configuration Control Boards, Architecture Review Board, and Investment Review Board.
- Ensure that an accurate IT systems inventory is established and maintained.
- Ensure that an IT security performance metrics program is developed, implemented, and funded.
- Advise the DHS CIO of any issues regarding infrastructure protection, vulnerabilities or issues that may cause public concern or loss of credibility.
- Ensure that incidents are reported to the DHS SOC within reporting time requirements as defined in Attachment F of the DHS Sensitive Systems Handbook
- Work with the DHS CIO and Public Affairs Office in preparation for public release of security incident information. *The DHS CIO, or designated representative, has sole responsibility for public release of security incident information.*

## **2.5 Chief Information Security Officer (CISO)**

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

The CISO:

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

- Ensures preparation and maintenance of plans and procedures to provide continuity of operations for information systems.

## **2.6 Office of the Chief Privacy Officer (CPO)**

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

The CPO serves as the senior official responsible for:

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

## **2.7 DHS Chief Security Officer (CSO)**

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

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

## **2.8 Component Information Systems Security Manager (ISSM)**

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

**ISSMs:**

- Oversee the Component IT security program.
- Ensure that IT security-related decisions and information, including updates to the 4300 series of IT security publications, are distributed to the ISSOs and other appropriate persons within their Component.
- Ensure that the Component CIO is kept apprised of all pertinent matters involving the security of IT systems.
- Approve and/or validate all Component IT system security reporting.
- Consult with the Component Privacy Office or Privacy Point of Contact (PPOC) for reporting and handling of privacy incidents.
- Manage IT security resources including oversight and review of Exhibit 300 funding documents.
- Review and approve the security of hardware and software prior to implementation into the Component SOC.
- Test the security of implemented systems periodically.
- Implement and manage the Plan of Action and Milestones (POA&M) process.
- Maintain an inventory of all IT systems.
- Ensure the Component IT security program is structured to support DHS and appropriate FISMA and OMB requirements.
- Develop and publish procedures necessary to implement the requirements of DHS IT security policy within the appropriate Component.
- Ensure that Information Systems Security Officers (ISSO) are appointed for each IT system managed at the Component level.
- Review and approve ISSO appointments.
- Ensure that the CISO-approved Risk Management System (RMS) automated tool is utilized for conducting certification and accreditation evaluations.
- Ensure that the CISO-approved Trusted Agent FISMA (TAF) automated tool is utilized for conducting self-assessment evaluations and for reporting required IT security program status information.
- Ensure that weekly incident reports are submitted to the DHS SOC.
- Acknowledge receipt of Information Security Vulnerability Management (ISVM) messages, report compliance with requirements or notify the granting of waivers.

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

The Component Privacy Offices and Privacy Points of Contact (PPOC) are responsible for compliance with Federal laws and DHS privacy policy at the Component level. The Privacy Officers and PPOCs work with the Component CIO and DHS CPO to maintain privacy

requirements. SOC's will work with their Component Privacy Offices, PPOCs, or with the DHS CPO to address suspected or confirmed privacy incidents (PI) or incidents involving PII.

Component Privacy Offices and Privacy Points of Contact will:

- Advise the Component CIO and management regarding privacy issues relevant to the Component.
- Receive and evaluate reports that impact DHS privacy programs.
- Work with system owners to complete privacy impact assessments
- Coordinate with program managers, Component ISSMs, CSIRC, or SOC in evaluating and reporting suspected or confirmed incidents involving PII.
- Inform the DHS CPO of the status of ongoing and completed privacy incidents in a timely manner.
- Advise the CPO regarding the handling of reported privacy Incidents.
- Provide privacy incident updates to US-CERT as further information is obtained.
- Work with the DHS CPO, Component CIO and Component CISO in preparation for release of computer security incident information involving PII or other privacy issues
- Work with the Component CIO and DHS Privacy Officer in preparation for release of computer security incident information involving PII or other privacy issues.

## **2.10 Program Manager (PM)**

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

Program Managers:

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

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

The United States Computer Emergency Readiness Team (US-CERT) is designated as the central reporting organization within the Federal Government and serves as the central repository for Federal incident data. The DHS SOC will report security incidents to the US-

CERT. The US-CERT may notify law enforcement, the Identity Theft Task Force, the Social Security Administration, and the Executive Office of the President, as appropriate.

## **2.12 Certifying Official**

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

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

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

## **2.13 Designated Accrediting Authority (DAA)**

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

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

DAAs:

- Review Notices of Findings and Recommendations (NFR) and Plans of Action and Milestones (POA&M)
- Review and approve corrective actions necessary to mitigate residual risks.
- Terminate system operation if security conditions warrant such action.

## **2.14 Information Systems Security Officer (ISSO)**

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

ISSOs:

- Serve as the principal points of contact for all IT security aspects pertaining to their systems.
- Work closely with the Component ISSM and DHS CISO staff to interpret and apply IT security policies and implementing procedures.
- Serve as liaison between system owners and the ISSM.
- Work with system owners to document weaknesses in POA&Ms and initiate corrective action.
- Employ automated tools (approved by the DHS CISO) such as the Risk Management System (RMS) and Trusted Agent FISMA (TAF).

## **2.15 System Owners**

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

System owners:

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

- Report Privacy and Computer Security incidents as appropriate, in coordination with the ISSM and Program Manager

## **2.16 Users of Supplied Computing Resources**

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

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

## **2.17 Additional Personnel**

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

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

## **2.18 DHS Chief Financial Officer designated Financial Systems**

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

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

### **2.18.1 DHS CFO**

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

- Identifying financial systems subject to OMB A-123 and Internal Controls over Financial Reporting (ICOFR) requirements (“CFO-designated financial systems”).
- Working with the Department CIO to ensure the confidentiality, integrity and availability of financial data processing.
- Overseeing the development and establishment of policies and procedures regarding automated application controls for Department-wide application software processing financial data.
- Remediating automated application control deficiencies related to financial application policies and procedures at the Department level.

- Tracking and monitoring progress of automated application controls corrective action plans and remediation efforts at the Department and Component Levels.
- Working with the Department CIO to identify and incorporate user requirements for new financial applications or existing Departmental financial applications.
- Working with the DHS CIO to integrate and test the Department-wide business continuity plan.
- Coordinating with the DHS CIO to identify the financial data to be backed up and recovered and developing policies to ensure that procedures are in place for backing up and recovering critical financial data.

### **2.18.2 DHS CIO**

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

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

### 2.18.3 Component CFO

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

- Works with the Component CIO and owners of CFO-designated financial systems to help ensure the reliability of financial data processing through Component systems.
- Develops and establishes policies and procedures regarding automated application controls for software processing of financial data.
- Remediates automated application controls deficiencies at the Component level.
- Works with system owners to designate an Information System Security Officer (ISSO) for each of the CFO-designated financial systems, as defined in Section 3.15 of DHS Sensitive Systems Policy Directive 4300A.
- Tracks and monitors progress of automated application controls remediation efforts at the Component level.
- Works with system owners of CFO-designated financial systems to ensure remediation of ITGC deficiencies related to IT policies and procedures.
- Approves accreditation of enterprise CFO-designated financial systems, if not already identified as the Designated Accrediting Authority (DAA). In this role, accept security risk identified during audits of CFO-designated financial systems, on behalf of the Department.
- Works with Component CIO to incorporate user requirements for new financial applications or upgrades to existing financial applications.
- Works with Component CIO to integrate and test Component-wide business continuity plan.
- Coordinates with Component CIOs to identify the financial data needed to be backed up and recovered.

### 2.18.4 Component CIO

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

- Reviews and evaluates the Component's CFO-designated financial systems to ensure ITGCs are in place and working effectively.
- Works with the system owners to ensure remediation of ITGC deficiencies related to CFO-designated financial systems.
- Tracks and monitors progress of ITGC POA&Ms and remediation efforts at the Component level.
- Ensures completion of Memorandums of Understanding (MOUs) and Interconnection Security Agreements (ISAs) for CFO-designated financial system interconnections with

any system not owned by DHS; ensures that they include appropriate security clauses; and monitors service provider for compliance with MOUs and ISAs.

- Implements the Department-wide system development lifecycle methodology and monitor user compliance with this methodology.
- As part of developing new financial applications or updating existing applications, integrates CFO feedback to ensure user requirements are adequately addressed.
- Develops and tests Component-wide disaster recovery plan. Coordinate with Component CFO to incorporate business continuity requirements and test on a periodic basis.
- Based on Component CFO requirements, executes policies for the routine backing up and recovery of financial data. Implements policies and procedures for rotating back-up media off-site.

### **2.18.5 System Owners**

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

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

### 3.0 MANAGEMENT CONTROLS

Management controls focus on management of the IT system (major application or general support system) itself and management of risk to that system. Examples include conducting risk assessments, developing rules of behavior, and ensuring that security is an integral part of the System Development Life Cycle (SDLC) and the Capital Planning and Investment Control (CPIC) processes. Management controls consist of techniques and concerns that are normally addressed by management personnel as indicated in the following sections.

#### 3.1 Basic Requirements

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

All security reports regarding DHS IT systems (major applications and general support systems) will be submitted by the ISSM to the Component Head or a designated representative. ISSMs will interpret and manage DHS security policies and procedures to meet Federal, Departmental, and Component requirements. They will also answer data queries from the Compliance and Oversight Program Director and develop and manage information security guidance and procedures unique to the Component's requirements. ISSOs are the primary points of contact for the security of the IT systems assigned to them. They develop and maintain System Security Plans and are responsible for overall system security.

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

Basic IT security responsibilities are provided below.

<b>Basic Requirements Responsibilities</b>
<p><b>System Owners</b></p> <ul style="list-style-type: none"> <li>• Appoint an ISSO for each IT system (see DHS 4300A Attachment C).</li> </ul> <p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Structure the Component-level IT Security Program to support DHS requirements.</li> <li>• Report all pertinent matters involving the security of IT systems to the head of the Component or a designated representative.</li> <li>• Interpret, tailor, implement, and manage DHS security policies and procedures to meet the Federal, Departmental, and Component requirements.</li> <li>• Develop, disseminate, implement, and manage IT security guidance and procedures unique to the Component's requirements.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Account for every DHS computing resource as part of a recognized IT system.</li> <li>• Develop and maintain a System Security Plan for each assigned IT system.</li> <li>• Serve as the POC on all security matters for each assigned IT system.</li> </ul>

### 3.2 Capital Planning and Investment Control

In accordance with the requirements of the Federal Information Security Management Act of 2002 (FISMA), annual agency budgets must address the adequacy and effectiveness of information security policies, procedures, and practices. This implies that security controls must be included in both capital planning and IT procurement actions for the current budget year and for the Future Years Homeland Security Program (FYHSP).

<b>DHS Policy</b>
<p><b>a.</b> System owners shall include IT security requirements in their capital planning and investment business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP).</p>
<p><b>b.</b> System owners or DAAs shall ensure that IT security requirements and POA&amp;Ms are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.</p>
<p><b>c.</b> Component Investment Review Boards (IRBs) shall not approve any capital investment in which the IT security requirements are not adequately defined and funded.</p>

Capital planning and investment control responsibilities are provided below.

<b>Capital Planning and Investment Control Responsibilities</b>
<p><b>DHS CIO</b></p> <ul style="list-style-type: none"> <li>• Coordinates the review of an independent evaluation of the DHS annual budget submission to ensure that IT security requirements are adequately addressed.</li> </ul> <p><b>ISSMs</b></p>

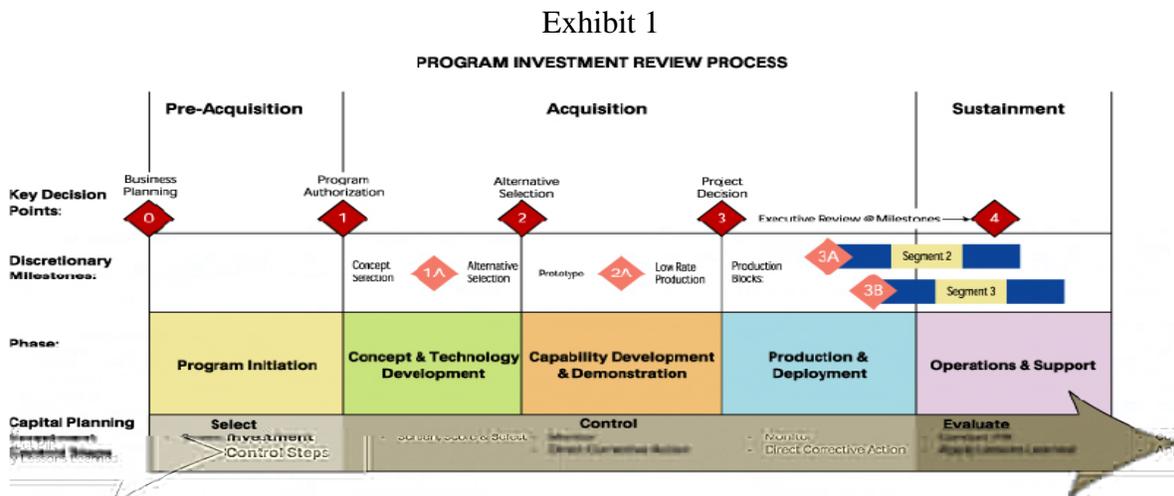
<b>Capital Planning and Investment Control Responsibilities</b>	
<ul style="list-style-type: none"> <li>• Ensure that IT security requirements are included in the organization’s capital planning and investment planning processes.</li> </ul>	
<b>System Owners</b>	
<ul style="list-style-type: none"> <li>• Ensure that funding for implementation of IT security is included in project life cycle planning.</li> </ul>	
<b>DAAs</b>	
<ul style="list-style-type: none"> <li>• Ensure that funding for implementation of IT security is included in project life cycle planning.</li> </ul>	

Two critical and complementary processes govern the management of IT within the DHS: Capital Planning and Investment Control (CPIC) and System Development Life Cycle (SDLC). A typical CPIC process is discussed in this section. SDLC processes and responsibilities are described in Section 3.6 below.

The protection of computer systems, networks, and data is essential to the effective management of IT resources. DHS security professionals thus play a key role in implementing both of these management processes. Senior managers must ensure that security considerations are adequately addressed in all aspects of DHS IT activities. This is accomplished by requiring all projects and programs to demonstrate through the SDLC documentation that they have met all appropriate security standards and criteria at specific points in their development and investment lifecycles as defined by the CPIC process. Programs that have not met the standards and criteria can be denied funding.

**Capital Planning and Investment Control Process**

DHS investment management is governed by DHS Management Directive 1400, *Investment Review Process*. This Directive requires that all IT investments be reviewed by the DHS Enterprise Architecture Board at each of 4 Key Decision Points (KDPs), Program Authorization, Alternative Selection, Project Decision, and Executive Review. Exhibit 1 shows how these KDPs are related to the CPIC phases and the SDLC phases.



**Program Authorization:** At this KDP, programs are responsible for demonstrating the results of operational analysis and identification of program requirements developed to define the new

capability required to satisfy a mission. With approval at KDP1, the initiative is (1) designated as a Level 1 acquisition, (2) directed to charter a major acquisition Integrated Product Team (IPT), (3) authorized to commence the Concept & Technology Development phase, and (4) entered into the budget process. Typically, the initiative will enter the Fiscal Year (FY)+2 budget to provide staff and funding to proceed.

**Alternative Selection:** At this KDP, the program is evaluated on the feasibility of the alternative solution it has selected. The program will present its evaluation of the feasibility of alternatives and provide a basis for assessing the relative merits of alternatives (e.g., advantages and disadvantages, degree of risk, life cycle cost, cost benefit). Promising alternative solutions are defined in terms of cost, schedule, and performance objectives; identification of interoperability, supportability, and infrastructure requirements; opportunities for tradeoffs; an overall acquisition strategy; and a test and evaluation strategy (including Development Test and Evaluation [DT&E], and Operational Test and Evaluation [OT&E]).

The Program Manager will submit an updated Exhibit 300 containing or based on items identified above. This information and associated presentations are used to monitor initiatives, direct corrective actions, and determine when the investment is ready to proceed to the next phase.

**Project Decision:** At this KDP, the review is focused on the feasibility of the preferred alternative and refining the solution prior to a full production commitment.

In preparation for KDP 3, the Program Manager will review and update documents prepared during previous phases and develop: (1) proposed Exit Criteria for the Production and Deployment Phase. The Program Manager will submit an updated Exhibit 300. This information and associated presentations are used to monitor initiatives, manage risks, and determine when the investment is ready to proceed to the next phase.

With approval at KDP 3, the investment is authorized to commence the Production and Deployment Phase, and the future year's program plan must be fully funded.

**Executive Review:** At KDP 4, a project is reviewed against its performance and costs goals. The results of this review will form the basis for decisions on whether the project should be enhanced, reengineered, or retired.

At each of these KDPs, the security function has a formal role as a specialty reviewer, advising the EAB on whether the project should be allowed to proceed based on how well security is addressed at each lifecycle phase.

### **3.3 Contractors and Outsourced Operations**

Computer security requirements must be incorporated in contractual documents involving the acquisition, development, and/or operations and maintenance of computer resources. This applies at the beginning of a project or acquisition and in all follow-on contracts or purchasing agreements involving the acquisition of computer resources. This includes hardware, software, maintenance, and other associated IT products and services.

The use of contractors is essential to the success of the DHS. Contractors fill a vital role in the daily operations of the Department. They have a responsibility to protect the information they possess and process. To ensure the security of the information in their charge, contractors must adhere to the same rules and regulations as Government employees.

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

Responsibilities for contractors and outsourced operations are provided below.

<b>Contractors and Outsourced Operations Responsibilities</b>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Establish and maintain a contractor and outsourced operations policy for the Component.</li> </ul> <p><b>System Owners/IT Project Managers</b></p> <ul style="list-style-type: none"> <li>• Ensure that computer security requirements are reviewed and included in all applicable statements of work and other contractual agreements throughout the System Development Life Cycle.</li> <li>• Ensure that basic security requirements are integrated into the software and procurement life cycle for project development.</li> <li>• Ensure that computer security requirements are specified in the system design and functional requirements documents, and other SDLC documents, as required.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Coordinate with the system owners to ensure that contractor and outsourced operations policy requirements are met.</li> </ul>

System owners and IT Project Managers must review and include computer security requirements in the Solicitation document *prior to the acquisition of IT assets or services*. Information security must be a key factor in the source selection process and weighted commensurate with the sensitivity and criticality of the data to be processed. The Statement of Work (SOW) for all contracts (both initial and follow-on) must address computer security requirements. If the solicitation includes the purchase of a commercial off-the-shelf (COTS) application or if the system being developed has a COTS component, the security aspects of the

COTS product must be analyzed and, if appropriate, must identify and include security requirements in the acquisition specifications.

For DHS IT projects, computer security costs must appear in the initial investment management business case and also in subsequent cost benefit analyses throughout the SDLC. At a minimum, the system design and functional requirements documents must include computer security requirements.

### 3.4 Performance Measures and Metrics

Note: This section will be updated to reflect the results of the current Balanced Scorecard Initiative.

A Department-wide security performance measures and metrics program will be developed for the DHS. Appropriate information on the program will be included in this section.

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

Performance measures and metrics responsibilities are provided below.

<b>Performance Measures and Metrics Responsibilities</b>
<p><b>CISO</b></p> <ul style="list-style-type: none"> <li>• Establishes an IT security metrics program for the DHS.</li> </ul> <p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Define performance metrics to evaluate the effectiveness of the IT security program.</li> <li>• Provide semiannual data on their Component's progress in meeting DHS's performance measures to the CISO.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Provide input to the identification and selection of specific performance metrics for their systems.</li> <li>• Identify sources of metrics data and assign personnel to gather chosen data.</li> <li>• Monitor metrics data collection and integrate/analyze data for reporting purposes.</li> <li>• Provide performance metrics information to the ISSMs as required.</li> </ul>

NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003, provides guidance on how an organization, through the use of metrics, can identify the adequacy of in-place security controls, policies, and procedures. NIST 800-55 describes an approach to assist management in determining where to invest resources in additional security protection or where to discontinue nonproductive controls. It explains a process to develop and implement metrics and how these metrics can be used to justify security control expenditures.

A security metrics program within an organization should be built with four interdependent components:

1. Strong upper-level management support
2. Practical security policies and procedures
3. Quantifiable performance metrics
4. Results-oriented metrics analysis.

IT security performance goals and objectives must be the basis for the security metrics that are established. IT security metrics monitor the success of these goals and objectives by quantifying the level of compliance of the security controls. NIST SP 800-55 provides examples of metrics.

When implementing an IT security metrics program, the metrics must yield information that can be quantified for comparison purposes, in order to track progress using the same points of reference. Percentages or averages are common, and absolute numbers may be useful, depending on the activity being measured. Data required for calculating metrics must be easily obtainable, and the process that is under consideration must be measurable. To be measurable, a repeatable process is required. Only processes that are performed in a relatively formal manner should be considered for measurement. Metrics data must be easily obtainable to ensure that the cost of data collection does not exceed the benefits derived from the collection and assessment process.

### **3.5 Continuity Planning for Critical DHS Assets**

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

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

The COOP planning element of this program requires DHS Components to develop, test, exercise, and maintain comprehensive plans so that essential DHS business functions can be continued following an emergency situation. COOP plans are business oriented and focus on sustaining an organization's essential functions at an alternate site until the primary site can be restored.

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

#### **3.5.1 Continuity of Operations Planning**

DHS must have the capability to ensure continuity of essential functions under all circumstances. In support of DHS Strategic Goals, COOP planning policies are designed to establish a DHS-wide capability to react to emergency events (**response**); restore essential business functions if a disruption occurs (**recovery**); and achieve a resumption of normal operations (**reconstitution**).

COOP planning focuses on sustaining an organization’s essential business functions at an alternate site until the primary site can be restored. This requires that DHS Components develop, test, exercise, and maintain comprehensive plans to ensure that essential DHS business functions can be continued off site following an emergency. These plans address three essential phases:

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

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

General COOP planning responsibilities are shown below. Specific COOP responsibilities for DHS Components are detailed in the DHS Headquarters Continuity of Operations Plan.

<b>Continuity of Operations Planning Responsibilities</b>
<p><b>DHS Continuity Planning Program Director</b></p> <ul style="list-style-type: none"> <li>• Administers the Continuity Planning for Critical DHS Assets Program. Develops, maintains, and promulgates program requirements.</li> <li>• Provides oversight and ensures program compliance across DHS Components.</li> <li>• Provides COOP planning guidelines to the Components.</li> <li>• Facilitates the development and testing of COOP plans.</li> <li>• Approves DHS COOP plans and maintains COOP status.</li> </ul> <p><b>Component ISSMs</b></p> <ul style="list-style-type: none"> <li>• Identify and align office functions with DHS essential functions.</li> <li>• Identify vital records, IT, and personnel requirements needed to recover office functions.</li> <li>• Administer the Component Continuity Planning program.</li> <li>• Ensure the development of the Component COOP plans. Ensure that COOP planning is implemented for each line of business.</li> <li>• Provide COOP status and strategy to the DHS Continuity Planning Program Director.</li> </ul>

<b>Continuity of Operations Planning Responsibilities</b>
<ul style="list-style-type: none"> <li>• Develop and maintain a Component COOP Multi-Year Strategy and Program Plan.</li> </ul> <p><b>Component ISSOs</b></p> <ul style="list-style-type: none"> <li>• Comply with the Component Continuity Planning program.</li> <li>• Perform continuity planning and testing and document results.</li> <li>• Assist in the development of the Component COOP Multi-Year Strategy and Program Plan.</li> <li>• Ensure operational security is maintained during any test or recovery activities.</li> </ul>






### **3.5.1.1 COOP Planning Requirement**

COOP planning is required by Presidential Decision Directive 67. Components are required to develop, test, exercise, and maintain Continuity of Operations (COOP) plans for the recovery of essential business functions identified in the DHS Headquarters COOP Plan. COOP plans are business oriented and thus focus on sustaining the essential functions of the organization (usually a headquarters element) and the supporting business functions (including those identified as national critical) at an alternate site and performing those functions for up to 30 days before returning to normal operations.

### **3.5.1.2 COOP Planning Objectives**

COOP planning is designed to achieve the following objectives:

- Ensure the continuous performance of DHS essential functions/operations during an emergency
- Protect equipment, vital records, and other assets to meet mission needs
- Reduce or mitigate disruptions to operations
- Reduce loss of life, minimizing damage and losses

Achieve a timely and orderly recovery from an emergency and resumption of full service to customers.

### **3.5.1.3 COOP Plan Content**

To facilitate their usefulness and acceptance by the users, COOP plans need to be brief and concise. COOP plans must encompass the following elements:

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

- Reconstitution (return to normal operations).

Because Continuity of Operations emphasizes the recovery of an organization's operational capability at an alternate site, the COOP plan will not necessarily address IT operations. COOP plans normally focus on facility-level and organization contingency planning rather than IT contingency planning. IT requirements are considered in the COOP plan in terms of their support of essential functions and the supporting office functions and should be documented in the COOP plan. Although IT contingency planning is a separate effort (see Section 3.5.3), these plans can be included in the COOP Plan as appendices. Close coordination with IT support operations is required to ensure IT availability at the alternate site(s).

#### 3.5.1.4 COOP Test, Training, and Exercise (TT&E)

The most important aspect of successful Continuity of Operations planning is the periodic testing and exercising of the COOP Plan. To demonstrate a viable continuity of operations capability, COOP plans must be periodically tested and exercised, and COOP personnel must be trained. Tests and exercises serve to validate specific aspects of COOP plans, policies, procedures, systems, and facilities that would be used during an emergency event. DHS Components are to conduct periodic TT&E, so that weaknesses in the COOP Plan can be identified and corrected. TT&E results must be documented.

### 3.5.2 IT Contingency Planning

IT contingency planning is an integral part of the Department of Homeland Security (DHS) Continuity Planning for Critical DHS Assets Program. Consequently, this policy supplements Continuity of Operations (COOP) Planning policy.

IT contingency planning is designed to ensure the availability of critical IT support under all circumstances. Components are required to develop, test, and maintain IT Contingency Plans to ensure adequate IT is available to sustain DHS essential and supporting office functions in accordance with the requirements for the FIPS 199 potential impact level for the availability security objective. See Section 3.9.1, *FIPS 199 Categorization and the NIST SP 800-53 Controls*, for more information on DHS's approach to system categorization.

In support of DHS strategic goals, IT contingency planning is designed to establish a DHS-wide capability to react to emergency events (**response**), restore essential business functions if a disruption occurs (**recovery**), and achieve a resumption of normal operations (**reconstitution**).

DHS Policy
<b>a.</b> Guidance, direction, and authority for IT contingency planning activities for all DHS Components are centralized in the DHS Office of the CIO.
<b>b.</b> To ensure critical IT system availability under all circumstances, a standard DHS-wide process for IT contingency planning shall be developed, documented, and maintained.
<b>c.</b> Components shall implement and enforce backup procedures for all sensitive IT systems, data, and information. Recommended intervals are daily for incremental data backups and weekly for full data backups. System and application software should be backed up whenever modifications to the

<b>DHS Policy</b>
software make backups necessary.
<b>d.</b> The rigor of the IT system contingency planning, training, testing and capabilities shall be dependent upon the FIPS 199 defined potential impact level. The <b>availability</b> security objective alone shall be applied to the NIST SP 800-53 contingency planning (CP) controls defined for the low, moderate, and high potential impact level systems.
<b>e.</b> Comprehensive IT Contingency Plans to continue and recover critical DHS major applications and general support systems shall be developed, tested, exercised, and maintained by all DHS Components in accordance with the requirements for the FIPS 199 potential impact level for the <b>availability</b> security objective. These plans shall be based on three essential phases: Activation/Notification, Recovery, and Reconstitution.
<b>f.</b> When testing is required, IT Contingency Plans shall be tested/exercised annually.
<b>g.</b> All personnel involved in IT contingency planning efforts shall be identified and trained in the procedures and logistics of IT contingency planning and implementation as required.
<b>h.</b> Personnel involved in IT contingency planning efforts shall receive IT Contingency Plan training or refresher training annually.

IT contingency planning responsibilities are provided below.

<b>IT Contingency Planning Responsibilities</b>
<p><b>DHS Continuity Planning Program Director</b></p> <ul style="list-style-type: none"> <li>• Administers the Continuity Planning for Critical DHS Assets Program. Develops, maintains, and promulgates program requirements.</li> <li>• Provides oversight and ensures program compliance across DHS Components.</li> <li>• Provides IT contingency planning guidelines to Component ISSMs.</li> <li>• Facilitates the development and testing of IT Contingency Plans.</li> <li>• Approves DHS IT Contingency Plans and maintains status.</li> </ul> <p><b>System/Network Administrators</b></p> <ul style="list-style-type: none"> <li>• Participate in all phases of the contingency planning process.</li> </ul> <p><b>Site Managers/System Owners</b></p> <ul style="list-style-type: none"> <li>• Ensure that the system's FIPS 199 potential impact for the availability security objective is correct and maintained to be consistent with system information processing changes.</li> <li>• Ensure that adequate resources are budgeted for contingency planning, testing, and training consistent with the availability objective of the system.</li> <li>• Ensure that adequate Contingency Plans are included in C&amp;A documentation.</li> </ul> <p><b>Component ISSMs</b></p> <ul style="list-style-type: none"> <li>• Establish Component continuity planning programs consistent with Department policy.</li> <li>• Provide IT contingency planning status and strategy to the DHS Continuity Planning Program</li> </ul>

<b>IT Contingency Planning Responsibilities</b>
<p>Director.</p> <p><b>Component ISSOs</b></p> <ul style="list-style-type: none"> <li>• Comply with the Component continuity planning program.</li> <li>• Ensure that the system's FIPS 199 potential impact for the availability security objective is consistent with the information types processed, stored, and transmitted by the system.</li> <li>• Ensure comprehensive IT Contingency Plans are developed, as required, for each major application and general support system under their purview.</li> <li>• Perform contingency planning, testing/exercising, and training, as required. For systems with moderate and high potential impact for availability, testing/exercising and training shall occur at least annually and when significant changes are made to the IT application or system, supported essential and office function(s), or the IT Contingency Plan. Examples of significant changes to information systems include installation of a new or upgraded operating system, middleware component, or application; modifications to system ports, protocols, or services; installation of a new or upgraded hardware platform or firmware component; or modifications to cryptographic modules or services.</li> <li>• Ensure operational security is maintained during any test or recovery activities.</li> </ul>



IT contingency planning represents a broad scope of activities designed to sustain and recover critical IT services following an emergency and includes identification of procedures and capabilities for recovering major applications and general support systems.

IT Contingency Plans are IT oriented and therefore focus on sustaining an organization's critical IT services provided by the major applications and general support systems that sustain essential and supporting office functions.

### 3.5.2.1 IT Contingency Planning Requirement

IT contingency planning is directed by (1) NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, (2) Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, and (3) NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*.

Appendix III requires the development and maintenance of continuity of support plans for general support systems and IT Contingency Plans for major applications. NIST SP 800-34 considers continuity of support planning to be synonymous with IT contingency planning. Because an IT Contingency Plan should be developed for each major application and general support system, multiple Contingency Plans may be maintained within the organization's Continuity of Operations (COOP) Plan or Business Continuity Plan.

NIST SP 800-53 defines a family of security controls for Contingency Planning (CP). It identifies the level that these controls should be developed for high, moderate, and low potential impact systems. DHS uses the FIPS 199 designation of the availability security objective to define the impact level applicable to contingency planning controls (see Section 3.9.1 for information on DHS guidance on FIPS 199 system categorization and implementation of the NIST SP 800-53 security controls).

### **3.5.2.2 IT Contingency Plan Development**

IT contingency planning is designed to achieve the following objectives:

- Ensure the continuous availability of the critical IT systems that support DHS essential office functions during an emergency
- Protect IT assets and vital records needed to support mission needs
- Reduce or mitigate disruptions to operations
- Reduce loss of life, minimizing damage and losses
- Achieve a timely and orderly recovery from an emergency and the resumption of full IT service to customers.

### **3.5.2.3 IT Contingency Plan Format and Content**

To facilitate their usefulness and acceptance by the users, IT Contingency Plans need to be brief and concise. The specific control requirements and level of effort are determined based on the IT system's security categorization. The level of resources for the Contingency Plan is based on the security categorization for the availability security objective. See Section 3.9.6, *Contingency Plan*, for more information on the Contingency Plan template requirements.

IT Contingency Plans must encompass the following elements as required for the potential impact level for the system's availability security objective:

- Disruption impacts and allowable outage times
- Preventive controls and recovery strategies
- Vital records
- Responsible personnel
- Alternate operating facilities
- Devolution of control (delegations of authority and orders of succession)
- Reconstitution (return to normal operations)

### **3.5.2.4 IT Contingency Plan Test and Exercise**

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

Contingency Plan testing requirements for systems at each impact level for availability are described in Section 3.9.8.1–3.9.8.3.

### **3.5.2.5 IT Contingency Plan Training**

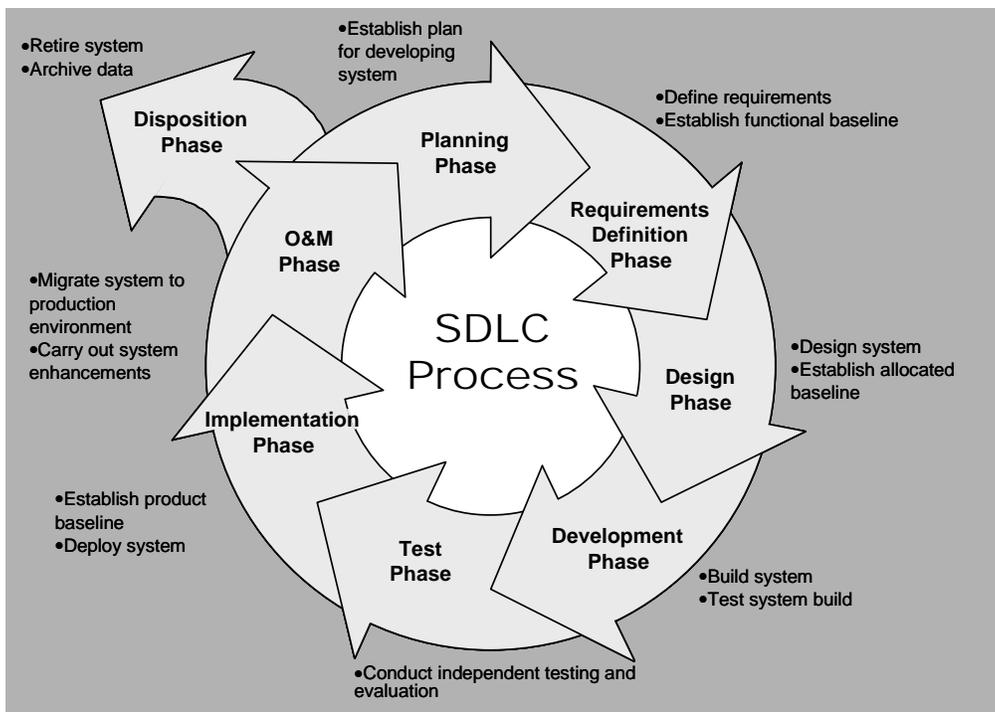
Training prepares recovery personnel for plan activation and improves plan effectiveness for overall agency preparedness. The IT system personnel shall be trained on the Contingency Plan according to the potential impact level of the availability security objective.

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

### 3.6 System Development Life Cycle

The SDLC methodology provides a structured approach to managing IT projects. It also allows introduction of IT security planning, including budgeting, review, and oversight. The SDLC process begins when the Program Authorization decision (discussed in Section 3.2) within a CPIC determines that an IT project should be initiated.

There are eight distinct phases in the SDLC as depicted in the figure below:



DHS Policy
a. Components shall ensure that system security is integrated into all phases of the System Development Life Cycle (SDLC).
b. Components shall ensure that security requirements for sensitive IT systems are incorporated into

<b>DHS Policy</b>
life-cycle documentation.
c. All custom developed code shall be reviewed, approved and signed by the Program Manager prior to deployment into production environments. The Program Manager may delegate this authority to another DHS employee in writing. This authority shall not be delegated to contractor personnel.

SDLC responsibilities are provided below.

<b>SDLC Responsibilities</b>
<p><b>CIO</b></p> <ul style="list-style-type: none"> <li>• Defines and promulgates the DHS SDLC process.</li> <li>• Ensures that IT security life cycle planning is integrated into DHS capital planning and investment control process.</li> </ul> <p><b>CISO</b></p> <ul style="list-style-type: none"> <li>• Ensures that IT security requirements are included in the DHS SDLC.</li> <li>• Oversees proper implementation of security controls in system development.</li> </ul> <p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Establish procedures for reviewing compliance with SDLC documentation requirements.</li> <li>• Participate in capital planning and investment management meetings involving SDLC considerations for IT systems and networks.</li> <li>• Ensure that required IT security documentation is produced and reviewed in accordance with SDLC milestones.</li> <li>• Approve IT security documentation produced as part of the SDLC process (except the C&amp;A package).</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Participate in planning and executing the SDLC process.</li> <li>• Provide IT security expertise to system development teams.</li> <li>• Review and comment on all SDLC security documents.</li> </ul> <p><b>System Owners/IT Project Managers</b></p> <ul style="list-style-type: none"> <li>• Ensure required security documents and reviews are included in the SDLC.</li> <li>• Ensure that adequate funding is available for implementation of security requirements.</li> <li>• Prepare required security documents.</li> </ul>












### 3.6.1 Planning

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

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

### **3.6.2 Requirements Definition**

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

- Updating the Risk Assessment and Security Plan
- Reviewing IT Baseline Security Requirements (DHS 4300A Attachment A)
- Reviewing IT Security budget requirements
- Preparing the initial security inputs to the IT Training Plan
- Preparing the initial Contingency Plan.

### **3.6.3 Design**

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

- Updating the Risk Assessment and Security Plan
- Reviewing budget requirements
- Updating the security information in the IT Training Plan
- Updating the Contingency Plan
- Preparing the initial Certification and Accreditation (C&A) package.

### **3.6.4 Development**

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

- Conducting the initial Developmental Security Test and Evaluation (ST&E)
- Updating the Risk Assessment and Security Plan
- Developing the initial Operational ST&E
- Reviewing budget requirements
- Updating the C&A package.

### **3.6.5 Test**

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

- Conducting formal Developmental ST&E
- Reviewing budget requirements
- Updating the Risk Assessment and Security Plan
- Updating the C&A package.

### **3.6.6 Implementation**

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

- Conducting the Operational ST&E on upgraded or new systems
- Reviewing adequacy of budget requirements
- Finalizing the security inputs in the IT Training Plans
- Updating the Risk Assessment and Security Plan
- Finalizing the Certification and Accreditation (C&A) package.

### **3.6.7 Operations and Maintenance**

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

- Reviewing C&A status and maintaining the currency of the C&A documentation
- Conducting annual user security awareness training and role-based training (e.g., training for ISSOs, DAAs, network and system administrators, managers)
- Maintaining adequate budgetary resources.

### **3.6.8 Disposition**

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

- Terminating system operations

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

### 3.7 Configuration Management

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

CM will apply to all systems, subsystems, and components of the DHS infrastructure, thereby ensuing implementation, and continuing life-cycle maintenance. CM begins with base lining of requirements documentation and ends with decommissioning of items no longer used for production or support.

The CM discipline will be applied to hardware, including power systems, software, firmware, documentation, test and support equipment, and spares. The Change Control Board (CCB) will ensure that documentation associated with an approved change to a DHS system is updated to reflect the appropriate baseline, including an analysis of any potential security implications. The initial configuration must be documented in detail and all subsequent changes must be controlled through a complete and robust CM process. Configuration management has security implications in three areas:

- Ensuring that the configuration of subordinate IT system elements are consistent with the certification and accreditation requirements of the parent system
- Ensuring that any subsequent changes, including an analysis of any potential security implications, are approved
- Ensuring that all recommended and approved security patches are properly installed

As new systems and newly modified systems proceed through the SDLC, changes to these systems must be documented and tested prior to placing these systems into the operational environment. This includes the testing of security controls. The objective is to ensure that new vulnerabilities are not introduced during the change process. The same requirements apply to operational systems as they undergo periodic modifications. Changes must be documented and tested prior to placing the system back into the operational environment.

Configuration management policies must take into account and have provisions for quickly testing and approving time-sensitive changes that result from newly released vulnerability information. Often in today's climate, severe new vulnerabilities quickly present themselves and the risk of not immediately implementing the vendor-supplied patches exceeds the risk of installing an untested vendor patch. DHS Components must have provisions for reacting quickly as these critical patches are identified and released by the DHS CSIRC.

<b>DHS Policy</b>
<p><b>a.</b> Components shall prepare configuration management plans for all IT systems, as part of their SSPs.</p>

<b>DHS Policy</b>
<p><b>b.</b> Components shall establish, implement, and enforce configuration management controls on all IT systems and networks and address significant deficiencies as part of a Plan of Action and Milestones (POA&amp;M).</p>
<p><b>c.</b> IT security patches must be installed in accordance with configuration management plans and within the timeframe or direction stated within the Information Security Vulnerability Management (ISVM) message published by the DHS Computer Security Incident Response Center (CSIRC).</p>

Configuration management responsibilities are provided below.

<b>Configuration Management Responsibilities</b>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Ensure that security issues are being addressed in configuration reviews and change control boards.</li> </ul> <p><b>Certifying Officials</b></p> <ul style="list-style-type: none"> <li>• Re-certify the system if significant configuration changes have been made.</li> </ul> <p><b>DAAs</b></p> <ul style="list-style-type: none"> <li>• Re-accredit their systems if significant configuration changes have been made.</li> <li>• Ensure that IT Project Managers and Development/O&amp;M Support Teams implement an effective configuration management process in accordance with SDLC requirements.</li> </ul> <p><b>Site Management</b></p> <ul style="list-style-type: none"> <li>• Ensures that approved configuration changes are correctly implemented at the site.</li> </ul> <p><b>IT Project Managers/ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that configuration management procedures are documented and implemented for all proposed configuration changes to IT systems.</li> <li>• Ensure that all proposed configuration changes to operating systems and applications are analyzed prior to implementation to determine if the proposed change has security implications.</li> <li>• Maintain a capability to quickly approve and implement time-sensitive security patches in reaction to late-breaking security vulnerabilities identified by the DHS CSIRC.</li> <li>• Ensure that all proposed configuration changes to operating systems, operating system security features, applications, critical system files, and system devices are formally approved, tested, and documented prior to the change being implemented.</li> <li>• Ensure that all approved changes to the configuration baseline are documented, reviewed for accuracy, and that records are maintained for each IT system for both the current and all previous configurations.</li> <li>• Ensure that formal system configuration reviews are performed.</li> <li>• Ensure that accurate system documentation and configuration logs are maintained to reflect current and prior configuration baselines.</li> <li>• Prepare and distribute a configuration management plan for each system under their authority.</li> <li>• Implement and enforce configuration management controls.</li> </ul> <p><b>Project Team</b></p>

<b>Configuration Management Responsibilities</b>
<ul style="list-style-type: none"> <li>• Understand and comply with the configuration management plan for the system.</li> <li>• Comply with configuration management controls and procedures.</li> </ul>



The Component ISSM will make determinations as to when time-sensitive system patches identified by DHS CSIRC must be quickly implemented to protect the Component's infrastructure. The ISSM, in cooperation with network operations leadership, will determine how quickly late-breaking patches must be expedited through the configuration management process and installed on DHS systems in order to protect mission accomplishment.

The ISSO and IT project manager work with the cognizant Development Team (for new development systems) or the Operations and Maintenance (O&M) Support Team (for fielded systems) to ensure that all proposed changes to the configuration baseline are analyzed and tested to determine if the proposed changes have security implications. As new vulnerabilities are identified during the testing process, appropriate security software patches must be developed and installed prior to implementation of the proposed change.

Any changes that impact the security posture of the system must be brought to the attention of the Certifying Official and the Designated Accrediting Authority (DAA). Further, all proposed configuration changes to operating systems, operating system security features, applications, critical system files, and system devices must then be formally approved and documented prior to the change being implemented. If the approved change is deemed to be significant, the C&A documentation must be updated.

This configuration management process continues throughout the life cycle of the system.

### **3.8 Risk Management**

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

The purpose of risk management is to identify risks, assess the impacts of the risks identified, and to take appropriate steps to reduce the identified risks to an acceptable level. An effective risk management process is a vital component of a successful IT security program. An organization's risk management process is designed to protect the *organization and its ability to perform its mission*, not just its IT assets.

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

- Better securing the IT systems that store, process, or transmit organizational information
- Enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget
- Assisting management in authorizing (or accrediting) IT systems on the basis of the supporting documentation resulting from the performance of risk management.

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

Risk management responsibilities are provided below.

<b>Risk Management Responsibilities</b>
<p><b>CISO</b></p> <ul style="list-style-type: none"> <li>• Establishes and enforces policy relating to the Risk Management process.</li> </ul>
<p><b>Certifying Officials</b></p> <ul style="list-style-type: none"> <li>• Evaluate the Risk Assessment document as part of the certification process.</li> <li>• Ensure that the Risk Assessment contains information required for C&amp;A.</li> <li>• Recommend to the DAA the possible implementation of additional risk mitigation actions that would mitigate existing residual risks.</li> </ul>
<p><b>DAAs</b></p> <ul style="list-style-type: none"> <li>• Determine the overall degree of acceptable risk based on the Component's mission requirements.</li> <li>• Determine whether the residual risk for the IT system being accredited is within tolerable limits.</li> <li>• Make a risk-based decision to (1) grant system accreditation, (2) grant an interim authorization to operate the system for a designated period of time (systems in development testing or prototypes only), or (3) deny system accreditation because the risks to the system are not at an acceptable level.</li> </ul>
<p><b>System Owners</b></p> <ul style="list-style-type: none"> <li>• Assist in determining the degree of acceptable residual risk based on the agency's mission requirements.</li> <li>• Review the Certification Package and ensure resources are provided to implement risk mitigation measures.</li> </ul>
<p><b>IT Project Managers/ISSOs</b></p> <ul style="list-style-type: none"> <li>• Conduct the initial Risk Assessment.</li> <li>• Ensure that the system security plan and risk assessment contain information required by certification activities and address all appropriate management, operational, and technical controls.</li> <li>• Initiate follow-on Risk Assessments if any significant changes to the system configuration or to the operational/threat environment have occurred, or every three years, whichever comes first.</li> </ul>

The Risk Management process described in NIST SP 800-30 contains three key elements: (1) risk assessment, (2) risk mitigation, and (3) evaluation and assessment. Risk Management is an

integral part of the Certification and Accreditation (C&A) process, which is discussed in Section 3.9.

### **3.8.1 Risk Assessment**

Risk Assessments are used to determine the extent of potential threats and risks associated with an IT system throughout its lifecycle. Based on the results of the Risk Assessment, appropriate security controls can be identified to reduce risks to an acceptable level during the risk mitigation phase. See Section 3.9.4 for more information on developing a Risk Assessment with the RMS automated tool.

NIST SP 800-30 identifies nine major activities to be conducted in the development of the Risk Assessment:

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation.

### **3.8.2 Risk Mitigation**

The Risk Mitigation element occurs after the Risk Assessment phase is complete. Risk Mitigation encompasses the prioritization, evaluation, and implementation of appropriate security controls identified during the Risk Assessment phase.

NIST SP 800-30 identifies seven major activities to be conducted as part of the Risk Mitigation phase:

1. Prioritize Actions
2. Evaluate Recommended Control Options
3. Conduct a Cost-Benefit Analysis
4. Select Appropriate Controls
5. Assign Implementation Responsibility
6. Develop an Implementation Plan
7. Implement Selected Controls.

### 3.8.3 Evaluation and Assessment

Risk Management is an ongoing process that will evolve over time as IT systems are updated and replaced with newer versions. New risks can surface and risks previously mitigated can re-surface as concerns.

For these reasons, DHS Components must conduct risk assessments whenever significant changes to the system configuration or to the operational/threat environment occur, or every 3 years, whichever comes first. The Risk Assessment is a key component of the Certification and Accreditation process discussed in the following section.

### 3.9 Certification and Accreditation, Remediation, and Reporting

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

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

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

NIST 800-37 describes the four phases of certification and accreditation. The artifacts required by the RMS automated C&A tool and by the TAF automated reporting tool are listed below by the phase in which each is generated:

- **Initiation Phase**
  - FIPS 199 Categorization (Section 3.9.1)
  - Privacy Impact Assessment (Section 3.9.2)
  - e-Authentication (Section 3.9.3)
  - Risk Assessment (Section 3.9.4)
  - System Security Plan (Section 3.9.5)
  - Contingency Plan (Section 3.9.6).
- **Certification Phase**
  - Security Test and Evaluation (ST&E) Plan (Section 3.9.7)

- Contingency Plan Testing (Section 3.9.8)
- Security Assessment Report (SAR) (Section 3.9.9)
- **Accreditation Phase**
  - Authorization to Operate (ATO) Letter (Section 3.9.10)—includes updated System Security Plan (SSP), Plan of Action and Milestones (POA&M), SAR
- **Continuous Monitoring Phase**
  - Annual Self-Assessments (Section 3.9.11)

Certification is the comprehensive testing and evaluation of the management, operational, and technical IT security features and of other safeguards of an IT system. Certification establishes the extent to which a particular IT design and implementation meet a specified set of security requirements. Certification primarily addresses software and hardware security safeguards, but it also considers procedural, physical, and personnel security measures employed to enforce IT security policy.

Accreditation covers the activities leading to the authorization of an IT system to process, store, and transmit information.

The DHS C&A process is governed by the following NIST publications:

- NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004
- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005
- NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, June 2007
- NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003
- NIST Special Publication 800-60, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*, and *Volume II: Appendixes to Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004
- Federal Information Processing Standards Publication (FIPS Pub) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

All IT systems (major applications, general support systems) are to undergo C&A. In some situations, a common controls (type accreditation) approach may be used for accrediting a system as defined by DHS and NIST guidance. Prior to starting a common controls-based C&A, agreement should be reached with the DAA to ensure a sufficient approach is performed. The DHS Office of Information Security can discuss common control approach, including sampling criteria, if such a system is identified. See DHS 4300A Attachment D for more information on type certification/accreditation.

In accordance with approved DHS IT security policy, the Risk Management System (RMS) automated tool developed by SecureInfo, Inc., will be used to produce C&A packages for all DHS IT systems. As of April 11, 2005, all IT systems shall be accredited using RMS.

As of June 1, 2006, Components no longer had the option within RMS of applying only the DHS 4300A requirements for C&A. Instead, for accreditations begun June 1, 2006, or later, Components have been required to apply the NIST 800-53 controls. Applying the NIST 800-53 controls requires that systems be categorized.

Artifacts generated during the accreditation process are uploaded into TrustedAgent FISMA (TAF), which supports the remediation process with its capability to manage the POA&M process and which generates quarterly reports and the required annual self-assessment.

The artifacts required by the RMS and TAF automated tools are listed below and are described in more detail in the remainder of this section:

- FIPS 199 Categorization
- PIA
- E-Authentication
- Risk Assessment
- System Security Plan (SSP)
- Contingency Plan
- Security Test and Evaluation (ST&E)
- Contingency Plan Testing
- Security Assessment Report (SAR)
- Authorization to Operate (ATO)—includes updated System Security Plan (SSP), Plan of Action and Milestones (POA&M), SAR
- Annual Self-Assessments

The DHS *Certification and Accreditation (C&A) Guidance for SBU Systems: Users Manual* provides detailed instructions on using DHS automated tools for accrediting IT systems, for tracking remediation activities, and for performing the required self-assessments and generating the required reports using the DHS automated tools.

<b>DHS Policy</b>
<p><b>a.</b> Components shall assign an impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability) and shall apply NIST 800-53 controls specific to the security objective at the determined impact level. Impact levels shall be assigned according to the standards set in FIPS Pub 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i>, and following the guidance from NIST SP 800-60, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>. DHS C&amp;A policy is based on guidance from NIST SP 800-37, <i>Guide for the Security Certification and Accreditation of Federal Information</i></p>

<b>DHS Policy</b>
<i>Systems.</i> [Note: See 4300A Sensitive Systems Handbook for information on the security objective(s) relevant to each of the NIST 800-53 controls.]
<b>b.</b> All Components shall implement NIST SP 800-53 security controls, using the FIPS Pub 200, <i>Minimum Security Requirements for Federal Information and Information Systems</i> methodology, based on the impact level established for each security objective (confidentiality, integrity, availability). A minimum impact level of “ <b>moderate</b> ,” shall be assigned and a risk-based assessment shall be performed to determine whether the confidentiality security objective warrants being assigned an impact level of “ <b>high</b> ,” for all CFO designated financial systems and for systems processing or hosting personally identifiable information (PII).
<b>c.</b> Components should pursue type C&A for IT resources that are under the same direct management control; have the same function or mission objective, operating characteristics, security needs, and that reside in the same general operating environment, or in the case of a distributed system, reside in various locations with similar operating environments. Type C&A will consist of a master C&A package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites.
<b>d.</b> The DAA for a system shall be identified in TrustedAgent FISMA. The Component CIO shall serve as the DAA when the system owner or an appropriate program official has not been named as the DAA.
<b>e.</b> Component ISSMs shall ensure that all new or major upgrades of existing sensitive IT systems and networks are formally certified through a comprehensive evaluation of their management, operational, and technical security features.
<b>f.</b> The certification, made as part of and in support of the accreditation process, shall determine the extent to which a particular design and implementation plan meets the DHS required set of security controls.
<b>g.</b> Component ISSMs shall ensure that a risk assessment is conducted whenever any modifications are made to sensitive IT systems, networks, or to their physical environments, interfaces, or user community. SSPs shall be updated and re-certification conducted if warranted.
<b>h.</b> Components shall accredit systems at initial operating capability and every 3 years thereafter, or whenever a major change occurs, whichever occurs first.
<b>i.</b> DAAs may grant an Interim Authorization to Operate (IATO) for systems that are undergoing development testing or are in a prototype phase of development. A system must be certified and accredited in an Authorization to Operate (ATO) letter prior to passing the Key Decision Point 3 milestone in the development life cycle. IATOs are not appropriate for operational systems. The DAA may grant an IATO for a maximum period of 6 (six) months and may grant 1 (one) 6 (six) month extension.
<b>j.</b> If the system is not fully accredited and has not received a full ATO by the end of the second and final IATO, the system shall not be deployed as an operational system.
<b>k.</b> As a result of IG auditing experience, components shall request concurrence from CISO for all

<b>DHS Policy</b>
accreditations for six months or less.
1. All DHS IT systems shall be accredited using the automated tools, TAF and RMS, approved by the DHS CISO.

Certification and accreditation responsibilities are provided below.

<b>Certification and Accreditation Responsibilities</b>
<p><b>CISO</b></p> <ul style="list-style-type: none"> <li>• Establishes and enforces policy relating to the C&amp;A process.</li> </ul> <p><b>Certifying Officials</b></p> <ul style="list-style-type: none"> <li>• Ensure that the System Security Plan, Security Test &amp; Evaluation, Contingency Plan, and Risk Assessment contain the information required for C&amp;A.</li> <li>• Prepare the certifier's statement, which reflects the state of the security controls, based on the results of the ST&amp;E.</li> <li>• Recommend to the DAA the possible implementation of additional risk mitigation actions that would mitigate the residual risks identified by the ST&amp;E.</li> <li>• Assemble the Certification Package that includes the certification findings, and transmit to the DAA.</li> <li>• Maintain files of Certification Packages for each IT system.</li> </ul> <p><b>DAA's</b></p> <ul style="list-style-type: none"> <li>• Determine degree of acceptable residual risk based on agency's mission requirements.</li> <li>• Review the state of the security controls for the system and the mission requirements of the agency.</li> <li>• Assess the correctness and effectiveness of security controls and identify the level of risk remaining (residual risk) for the system in performing its operational mission.</li> <li>• Determine whether the residual risk is within tolerable limits.</li> <li>• Make a risk-based decision to (1) grant system accreditation, (2) grant an interim authorization to operate the system for a designated period of time (systems in development testing or prototypes only), or (3) deny system accreditation because the risks to the system are not at an acceptable level.</li> </ul> <p><b>System Owners</b></p> <p>Certification Responsibilities:</p> <ul style="list-style-type: none"> <li>• Ensure that adequate resources are budgeted for and allocated to the C&amp;A process.</li> <li>• Review the results of the Initiation and Security Certification phases and ensure resources are provided to identify and implement risk mitigation measures.</li> </ul> <p>Accreditation Responsibilities:</p> <ul style="list-style-type: none"> <li>• Assist in determining degree of acceptable residual risk based on agency's mission requirements.</li> <li>• Review the Certification Package and ensure resources are provided to implement risk mitigation measures.</li> </ul> <p><b>IT Project Managers/ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that the SecureInfo RMS automated tool is utilized to develop C&amp;A packages.</li> </ul>

### Certification and Accreditation Responsibilities

#### Certification Responsibilities:

- Ensure that the Security Plan and Risk Assessment contain information required by certification activities.
- Develop the ST&E plan, conduct the ST&E, and prepare the ST&E Report.

#### Accreditation Responsibilities:

- Complete the final Risk Assessment, update the Security Plan, prepare the certification findings, and prepare a Draft Certification Statement.
- Complete the Certification Package and forward to the Certifying Official.
- Maintain files of the Certification Package.
- Initiate Re-Accreditation activities if any significant changes to the system configuration or to the operational/threat environment that might affect system security have occurred, or every 3 years, whichever comes first.

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

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

At DHS, the necessary security controls, supporting the security objectives, required for an IT system will be implemented without the requirement to implement extra controls that may not be necessary. This is the minimum DHS standard; however, any program that wishes to implement more than the minimum controls can still implement them when appropriate. This policy amplification is a Department-level risk-based decision that is consistent with FISMA policy which requires DHS to “cost-effectively reduce information security risks to an acceptable level.” The tailoring of controls and use of compensating controls is also consistent with providing the safeguards necessary to reduce the risks in a specific operational environment.

This policy amplification is also consistent with the NIST information security guidance which promulgates the “concept of risk based decisions.” The due diligence required by FIPS 199 of determining the exact impact level each type of information contained on the system, and each of the security objectives, will lead to well defined impact levels for confidentiality, integrity, and availability of the system as a whole. It is important, when using a risk-based decision to minimize the security controls, that all of the information and the risks to that information be clearly defined and documented. In that way, the DAA can make an informed decision on the level of risk that is acceptable for the system and its information in the specific operational environment.

As a result, in the DHS FIPS 199 Workbook (developed from FIPS 199, NIST SP 800-60, and the DHS Business Reference Model), impact levels (high, moderate, low) can be assigned to each security objective. This means, for example, that a system with low risk availability, high risk integrity, and low risk confidentiality will not be required to implement all high controls across the board. Rather the controls that fall out of the analysis will be implemented (i.e., high

levels for integrity controls, low for the confidentiality and availability controls). NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, should be applied specific to the security objective determined impact level.

For systems involving personally identifiable information, the confidentiality security objective shall be assigned an impact level of at least moderate. A risk-based assessment shall be performed to determine whether the confidentiality security objective warrants being assigned an impact level of high for such systems.

The table below identifies the security objective(s) (C = confidentiality, I = integrity, and A = availability) assigned to each NIST 800-53 control by impact level (L = low, M = moderate, and H = high; a bullet indicates the control is applicable, and a check indicates the enhancement to the control is applicable). DHS 4300A Attachment M lists the NIST 800-53 controls by impact level and by security objective, and it provides information on the possible tailoring of these controls and on the use of compensating controls.

### NIST SP 800-53 Security Controls and DHS-assigned Security Objectives

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
<b>Access Control (AC)</b>					
AC-1	Access Control Policy and Procedures	CIA	●	●	●
AC-2	Account Management	C	●	●	●
	E1: Automated mechanisms for management of accounts	C	---	✓	✓
	E2: Automatic termination of temporary and emergency accounts	C	---	✓	✓
	E3: Automatic disabling of inactive accounts	C	---	✓	✓
	E4: Automated mechanisms for auditing actions on accounts	C	---	✓	✓
AC-3	Access Enforcement	C	●	●	●
	E1: Access to security functions and information is restricted to authorized personnel	C	---	✓	✓
AC-4	Information Flow Enforcement	C	---	●	●
	E1: Explicit labels	C	---	---	---
	E2: Protected processing domains	C	---	---	---
	E3: Dynamic security policy mechanisms	C	---	---	---
AC-5	Separation of Duties	C	---	●	●
AC-6	Least Privilege	C	---	●	●
AC-7	Unsuccessful Login Attempts	C	●	●	●
	E1: Automatic locking of account/node	C	---	---	---
A-8	System Use Notification	C	●	●	●

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
A-9	Previous Logon Notification	C	---	---	---
AC-10	Concurrent Sessions Control	C	---	---	●
AC-11	Session Lock	C	---	●	●
AC-12	Session Termination	C	---	●	●
	E1: Local and remote session termination	C	---	---	✓
AC-13	Supervision and Review — Access Control	C	●	●	●
	E1: Automated mechanisms to facilitate review of user activities	C	---	✓	✓
AC-14	Permitted Actions without Identification or Authentication	CI	●	●	●
	E1: Actions permitted only to necessary extent	CI	---	✓	✓
AC-15	Automated Marking	C	---	---	●
AC-16	Automated Labeling	C	---	---	---
AC-17	Remote Access	C	●	●	●
	E1: Automated mechanisms for monitoring and control of remote access	C	---	✓	✓
	E2: Encryption for protecting confidentiality of remote access sessions	C	---	✓	✓
	E3: Remote access controlled through a managed access control point.	C	---	✓	✓
	E4: Remote access for privileged functions	C	---	✓	✓
AC-18	Wireless Access Restrictions	C	●	●	●
	E1: Authentication and encryption for protecting wireless access to the information system	C	---	✓	✓
	E2: Scanning for unauthorized wireless access points	C	---	---	✓
AC-19	Access Control for Portable and Mobile Devices	C	---	●	●
AC-20	Use of External Information Systems	C	●	●	●
	E1: Prohibit use of external information system-to-access	C	---	✓	✓
<b>Awareness and Training (AT)</b>					
AT-1	Security Awareness and Training Policy and Procedures	CIA	●	●	●
AT-2	Security Awareness	CIA	●	●	●
AT-3	Security Training	CIA	●	●	●
AT-4	Security Training Records	CIA	●	●	●
AT-5	Contacts with Security Groups and Associations	CIA	---	---	---

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
<b>Audit and Accountability (AU)</b>					
AU-1	Audit and Accountability Policy and Procedures	CIA	●	●	●
AU-2	Auditable Events	CIA	●	●	●
	E1: Multi-component, system-wide audit trail	CIA	---	---	✓
	E2: Selected events audit	CIA	---	---	✓
	E3: Review and update auditable events	CIA	---	✓	✓
AU-3	Content of Audit Records	CIA	●	●	●
	E1: Detailed info. audit	CIA	---	✓	✓
	E2: Centrally managed audit	A	---	---	✓
AU-4	Audit Storage Capacity	IA	●	●	●
AU-5	Response to Audit Processing Failures	IA	●	●	●
	E1: Alert for max. capacity	A	---	---	✓
	E2: Real-time alert for audit failure events		---	---	✓
AU-6	Audit Monitoring, Analysis, and Reporting	CIA	---	●	●
	E1: Automated audit monitoring	CIA	---	---	✓
	E2: Alert for unusual activities	CIA	---	✓	✓
AU-7	Audit Reduction and Report Generation	IA	---	●	●
	E1: Report select criteria	IA	---	✓	✓
AU-8	Time Stamps	I	●	●	●
	E1: Synchronization of internal clocks	I	---	✓	✓
AU-9	Protection of Audit Information	CI	●	●	●
	E1: Audit on write-once media	I	---	---	---
AU-10	Non-Repudiation	I	---	---	---
AU-11	Audit Record Retention	A	●	●	●
<b>Certification, Accreditation, and Security Assessments (CA)</b>					
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	CIA	●	●	●
CA-2	Security Assessments	CIA	●	●	●
CA-3	Information System Connections	C	●	●	●
CA-4	Security Certification	CIA	●	●	●
	E1: Independent security control assessment	CIA	---	✓	✓
CA-5	Plan of Action and Milestones	CIA	●	●	●
CA-6	Security Accreditation	CIA	●	●	●
CA-7	Continuous Monitoring	CIA	●	●	●
	E1: Independent monitoring of security controls	CIA	---	---	---

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
<b>Configuration Management (CM)</b>					
CM-1	Configuration Management Policy and Procedures	CIA	●	●	●
CM-2	Baseline Configuration	IA	●	●	●
	E1: Update baseline at new installation	IA	---	✓	✓
	E2: Automated update of baseline configuration	IA	---	---	✓
CM-3	Configuration Change Control	CIA	---	●	●
	E1: Automated change control	CIA	---	---	✓
CM-4	Monitoring Configuration Changes	CIA	---	●	●
CM-5	Access Restrictions for Change	CIA	---	●	●
	E1: Automated access control	CIA	---	---	✓
CM-6	Configuration Settings	CI	●	●	●
	E1: Automated central configuration control	I	---	---	✓
CM-7	Least Functionality	CIA	---	●	●
	E1: Reviews functionality	CIA	---	---	✓
CM-8	Information System Component Inventory	CIA	●	●	●
	E1: Maintenance of information system components inventory	CIA	---	✓	✓
	E2: Automated mechanisms to maintain inventory	CIA	---	---	✓
<b>Contingency Planning (CP)</b>					
CP-1	Contingency Planning Policy and Procedures	CIA	●	●	●
CP-2	Contingency Plan	A	●	●	●
	E1: Coordinated plans	A	---	✓	✓
	E2: Capacity planning	A	---	---	✓
CP-3	Contingency Training	A	---	●	●
	E1: Simulated events training	A	---	---	✓
	E2: Automated training	A	---	---	---
CP-4	Contingency Plan Testing and Exercises	A	---	●	●
	E1: Coordinated testing	A	---	✓	✓
	E2: Alternate processing site testing	A	---	---	✓
	E3: Automated testing	A	---	---	---
CP-5	Contingency Plan Update	A	●	●	●
CP-6	Alternate Storage Site	A	---	●	●
	E1: Geographically separate	A	---	✓	✓
	E2: Pre-configured storage	A	---	---	✓
	E3: Identified access problems	A	---	✓	✓

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
CP-7	Alternate Processing Sites	A	---	●	●
	E1: Geographically separate	A	---	✓	✓
	E2: Identified access problems	A	---	✓	✓
	E3: Priority service contract	A	---	✓	✓
	E4: Pre-configured alternate site	A	---	---	✓
CP-8	Telecommunications Services	A	---	●	●
	E1: Priority service contract	A	---	✓	✓
	E2: No shared point of failure	A	---	✓	✓
	E3: Geographically separate	A	---	---	✓
	E4: Contingency plans for vendor services	A	---	---	✓
CP-9	Information System Backup	A	●	●	●
	E1: Backup tested	A	---	✓	✓
	E2: Backup restored in testing	A	---	---	✓
	E3: Separate backup facility or fire-rated container	A	---	---	✓
	E4: Protect from unauthorized modification	A	---	✓	✓
CP-10	Information System Recovery and Reconstitution	A	●	●	●
	E1: Recovery and Reconstitution testing	A	---	---	✓
<b>Identification and Authentication (IA)</b>					
IA-1	Identification and Authentication Policy and Procedures	CIA	●	●	●
IA-2	User Identification and Authentication	C	●	●	●
	E1: Multifactor authentication	C	---	✓	---
	E2: Multifactor authentication for local system access	C	---	---	✓
	E3: Multifactor authentication for remote system access	C	---	---	✓
IA-3	Device Identification and Authentication	C	---	●	●
IA-4	Identifier Management	C	●	●	●
IA-5	Authentication Management	C	●	●	●
IA-6	Authenticator Feedback	C	●	●	●
IA-7	Cryptographic Module Authentication	C	●	●	●
<b>Incident Response (IR)</b>					
IR-1	Incident Response Policy and Procedures	CIA	●	●	●
IR-2	Incident Response Training	CIA	---	●	●
	E1: Simulated events	CIA	---	---	✓
	E2: Automated response training	CIA	---	---	---

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
IR-3	Incident Response Testing and Exercises	CIA	---	●	●
	E1: Automated testing	CIA	---	---	✓
IR-4	Incident Handling	CIA	●	●	●
	E1: Automated handling	CIA	---	✓	✓
IR-5	Incident Monitoring	CIA	---	●	●
	E1: Automated tracking and analysis	CIA	---	---	✓
IR-6	Incident Reporting	CIA	●	●	●
	E1: Automated reporting	CIA	---	✓	✓
IR-7	Incident Response Assistance	CIA	●	●	●
	E1: Automated distribution	CIA	---	✓	✓
<b>Maintenance (MA)</b>					
MA-1	System Maintenance Policy and Procedures	CIA	●	●	●
MA-2	Periodic Maintenance	A	●	●	●
	E1: Maintenance logs	A	---	✓	✓
	E2: Automated schedules	A	---	---	✓
MA-3	Maintenance Tools	IA	---	●	●
	E1: Inspection of tools	CIA	---	---	✓
	E2: Malicious code check of tools	CIA	---	---	✓
	E3: Equipment sanitized	C	---	---	✓
	E4: Automated personnel check	C	---	---	---
MA-4	Remote Maintenance	CIA	●	●	●
	E1: Audit and review	CIA	---	✓	✓
	E2: Diagnostics in SSP	CIA	---	✓	✓
	E3: Level of security equal for diagnostic service	CIA	---	---	✓
MA-5	Maintenance Personnel	C	●	●	●
MA-6	Timely Maintenance	A	---	●	●
<b>Media Protection (MP)</b>					
MP-1	Media Protection Policy and Procedures	CIA	●	●	●
MP-2	Media Access	C	●	●	●
	E1: Guards or automated access control to media storage	C	---	✓	✓
MP-3	Media Labeling	C	---	---	●
MP-4	Media Storage	C	---	●	●
MP-5	Media Transport	C	---	●	●
	E1: Protection of media during transport	C	---	✓	✓

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
	E2: Information system media transport activities	C	---	✓	✓
	E3: Custodian to transport information system media	C	---	---	✓
MP-6	Media Sanitization and Disposal	C	●	●	●
	E1: Sanitization and disposal activities	C	---	---	✓
	E2: Test sanitization equipment and procedures	C	---	---	✓
<b>Physical and Environmental Protection (PE)</b>					
PE-1	Physical and Environmental Protection Policy and Procedures	CIA	●	●	●
PE-2	Physical Access Authorizations	C	●	●	●
PE-3	Physical Access Control	C	●	●	●
	E1: Physical access to information system	C	---	---	✓
PE-4	Access Control for Transmission Medium	C	---	---	●
PE-5	Access Control for Display Medium	C	---	●	●
PE-6	Monitoring Physical Access	CIA	●	●	●
	E1: Intrusion alarms and surveillance	CIA	---	✓	✓
	E2: Response to alarms	CIA	---	---	✓
PE-7	Visitor Control	C	●	●	●
	E1: Escort and monitor visitors	C	---	✓	✓
PE-8	Access Records	C	●	●	●
	E1: Automated review	CA	---	---	✓
	E2: Record of physical access	C	---	---	✓
PE-9	Power Equipment and Power Cabling	A	---	●	●
	E1: Redundant parallel cabling	A	---	---	---
PE-10	Emergency Shutoff	A	---	●	●
	E1: Accidental or unauthorized activation	A	---	---	✓
PE-11	Emergency Power	IA	---	●	●
	E1: Long-term alternate power	A	---	---	✓
	E2: Long-term, self-contained power	A	---	---	---
PE-12	Emergency Lighting	A	●	●	●
PE-13	Fire Protection	A	●	●	●
	E1: Suppression and detection	A	---	✓	✓
	E2: Alert responders	A	---	✓	✓
	E3: Automatic fire suppression	A	---	✓	✓
PE-14	Temperature and Humidity	A	●	●	●
PE-15	Water Damage Protection	A	●	●	●

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
	E1: Automatic water shut-off	A	---	---	✓
PE-16	Delivery and Removal	C	●	●	●
PE-17	Alternate Work Site	A	---	●	●
PE-18	Location of Information System Components	CIA	---	●	●
	E1: Location planning	CIA	---	---	✓
PE-19	Information Leakage	C	---	---	---
<b>Planning (PL)</b>					
PL-1	Security Planning Policy and Procedures	CIA	●	●	●
PL-2	System Security Plan	CIA	●	●	●
PL-3	System Security Plan Update	CIA	●	●	●
PL-4	Rules of Behavior	CIA	●	●	●
PL-5	Privacy Impact Assessment	C	●	●	●
PL-6	Security-Related Activity Planning	CIA	---	●	●
<b>Personnel Security (PS)</b>					
PS-1	Personnel Security Policy and Procedures	CIA	●	●	●
PS-2	Position Categorization	CIA	●	●	●
PS-3	Personnel Screening	C	●	●	●
PS-4	Personnel Termination	CA	●	●	●
PS-5	Personnel Transfer	C	●	●	●
PS-6	Access Agreements	C	●	●	●
PS-7	Third-Party Personnel Security	CIA	●	●	●
PS-8	Personnel Sanctions	CIA	●	●	●
<b>Risk Assessment (RA)</b>					
RA-1	Risk Assessment Policy and Procedures	CIA	●	●	●
RA-2	Security Categorization	CIA	●	●	●
RA-3	Risk Assessment	CIA	●	●	●
RA-4	Risk Assessment Update	CIA	●	●	●
RA-5	Vulnerability Scanning	CIA	---	●	●
	E1: Scanning tools update vulnerabilities	CIA	---	---	✓
	E2: Updates to reported list	CIA	---	---	✓
	E3: Ensure adequate scan coverage	CIA	---	---	---
<b>System and Services Acquisition (SA)</b>					
SA-1	System and Services Acquisition Policy and Procedures	CIA	●	●	●
SA-2	Allocation of Resources	CIA	●	●	●

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
SA-3	Life Cycle Support	CIA	●	●	●
SA-4	Acquisitions	CIA	●	●	●
	E1: Details on functional properties of security controls	CIA	---	✓	✓
	E2: Details on design and implementation of security controls	CIA	---	---	---
SA-5	Information System Documentation	CIA	●	●	●
	E1: Details for analysis/testing	CIA	---	✓	✓
	E2: Details on interfaces	CIA	---	---	✓
SA-6	Software Usage Restrictions	IA	●	●	●
SA-7	User Installed Software	CIA	●	●	●
SA-8	Security Engineering Principles	CIA	---	●	●
SA-9	External Information System Services	CIA	●	●	●
SA-10	Developer Configuration Management	CIA	---	---	●
SA-11	Developer Security Testing	CIA	---	●	●
<b>System and Communications Protection (SC)</b>					
SC-1	System and Communications Protection Policy and Procedures	CIA	●	●	●
SC-2	Application Partitioning	CI	---	●	●
SC-3	Security Function Isolation	I	---	---	●
	E1: Hardware separation	I	---	---	---
	E2: Divides security functions	I	---	---	---
	E3: Minimize non-security functions in isolation	I	---	---	---
	E4: Independent modules	I	---	---	---
	E5: Layered structure	I	---	---	---
SC-4	Information Remnance	CI	---	●	●
SC-5	Denial of Service Protection	A	●	●	●
	E1: Restriction of user launch	A	---	---	---
	E2: Limits info. flooding	A	---	---	---
SC-6	Resource Priority	A	---	---	---
SC-7	Boundary Protection	C	●	●	●
	E1: Separate subnets for public access	C	---	✓	✓
	E2: Prevent public access	C	---	✓	✓
	E3: Limit access points	C		✓	✓
	E4: Managed interface with external	C	---	✓	✓

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
	telecommunication service				
	E4: Deny network traffic by default	C	---	✓	✓
	E5: Unauthorized release of information	C	---	---	✓
SC-8	Transmission Integrity	I	---	●	●
	E1: Cryptographic to ensure recognition of changes	I	---	---	✓
SC-9	Transmission Confidentiality	C	---	●	●
	E1: Cryptographic to prevent unauthorized disclosure	C	---	---	✓
SC-10	Network Disconnect	CIA	---	●	●
SC-11	Trusted Path	CI	---	---	---
SC-12	Cryptographic Key Establishment and Management	IA	---	●	●
SC-13	Use of Cryptography	CI	●	●	●
SC-14	Public Access Protections	I	●	●	●
SC-15	Collaborative Computing	C	---	●	●
	E1: Physical disconnect	C	---	---	---
SC-16	Transmission of Security Parameters	C	---	---	---
SC-17	Public Key Infrastructure Certificates	CI	---	●	●
SC-18	Mobile Code	CIA	---	●	●
SC-19	Voice Over Internet Protocol	CIA	---	●	●
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	CIA	---	●	●
	E1: Security status of child subspaces	CIA	---	---	---
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	CIA	---	---	●
	E1: Data origin authentication and data integrity verification	CIA	---	---	---
SC-22	Architecture and Provisioning for Name/Address Resolution Service	CIA	---	●	●
SC-23	Session Authenticity	CIA	---	●	●
<b>System and Information Integrity (SI)</b>					
SI-1	System and Information Integrity Policy and Procedures	CIA	●	●	●
SI-2	Flaw Remediation	I	●	●	●
	E1: Central auto-updates flaws	I	---	---	✓
	E2: Remediation reports	I	---	✓	✓
SI-3	Malicious Code Protection	CIA	●	●	●
	E1: Central virus protection	I	---	✓	✓

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
	E2: Automatic updates	I	---	✓	✓
SI-4	Intrusion Detection Tools and Techniques	CIA	---	●	●
	E1: System-wide detections	CIA	---	---	---
	E2: Automated real-time analysis	CIA	---	---	✓
	E3: Automated reconfiguration	CIA	---	---	---
	E4: Monitor outbound traffic	CIA	---	✓	✓
	E5: Real-time alert for compromise	CIA	---	---	✓
SI-5	Security Alerts and Advisories	CIA	●	●	●
	E1: Automated advisories	CIA	---	---	✓
SI-6	Security Functionality Verification	IA	---	---	●
	E1: Alert of failed security test	CIA	---	---	---
	E2: Distributed security testing	I	---	---	---
SI-7	Software and Information Integrity	I	---	---	●
	E1: Integrity scans	I	---	---	✓
	E2: Automated tools	I	---	---	✓
	E3: Verification tools	I	---	---	---
SI-8	Spam Protection	CIA	---	●	●
	E1: Centrally managed	IA	---	---	✓
	E2: Automated updates	IA	---	---	---
SI-9	Information Input Restrictions	C	---	●	●
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	I	---	●	●
SI-11	Error Handling	CIA	---	●	●
SI-12	Information Output Handling and Retention	C	---	●	●

### 3.9.2 Privacy Impact Assessment (PIA)

IT systems involving personally identifiable information are required by Section 208 of the E-Government Act to have a Privacy Impact Assessment (PIA). A Privacy Threshold Analysis (PTA) is first performed to determine whether potential privacy data is being processed or stored by the IT system. Systems that are determined to have privacy concerns require a formal PIA.

The template for the Privacy Threshold Analysis is available on the CISO page of DHS Online; the template is also available through the DHS Privacy Office, and the DHS Compliance Help Desk (1-877-695-6955) can also provide assistance in obtaining the template for the Privacy Threshold Analysis. The PTA template is also included in the RMS tool.

The PIA template for those systems involving privacy information and requiring a PIA is available in the RMS tool. A Microsoft Word template is also available by contacting the DHS Compliance Help Desk.

The DHS *Certification and Accreditation (C&A) Guidance for SBU Systems: Users Manual* provides detailed information on the Privacy Threshold Analysis and on the PIA process.

### **3.9.3 E-Authentication**

E-Authentication security requirements must be applied to IT systems that allow online transactions. The first step is to determine whether Government e-authentication security requirements apply to the system. For those systems for which e-authentication security requirements apply, two additional steps are required:

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

The E-Authentication Workbook and the instructions needed for completing the workbook (see *DHS Information Security Categorization Guide*) are available on the CISO page of DHS Online. The DHS Compliance Help Desk (1-877-695-6955) can also provide assistance in obtaining these documents.

### **3.9.4 Risk Assessment**

Risk Assessment is the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. An initial risk assessment is used to understand the unique system risks and to determine if any controls are required to address specific threats or weaknesses to the system. The initial risk assessment incorporates system characterization information, security categorization determination (see Section 3.9.1), privacy threshold analysis and Privacy Impact Assessment (PIA) (Section 3.9.2), and e-Authentication assessment (Section 3.9.3). DHS follows the overall risk process as described in NIST Special Publication 800-30, *Risk Management Guide for IT Systems*. The results of the risk assessment will be used to directly address the controls that will be documented in the SSP and implemented within the system.

The initial Risk Assessment is updated and revised and becomes the final Risk Assessment as part of the overall accreditation process after the controls are implemented and tested and the results/corrective actions are implemented. Through the development of the final Risk Assessment, the definition of the program residual risk can be determined for the DAA's acceptance during accreditation.

An initial Risk Assessment document is generated within RMS when a C&A package is created and the questionnaire is run.

The DHS *Certification and Accreditation (C&A) Guidance for SBU Systems: Users Manual* provides detailed information on developing the Risk Assessment within RMS.

### **3.9.5 System Security Plan (SSP)**

The System Security Plan (SSP) provides a complete description of the information system, including purposes and functions, system boundaries, architecture, user groups, interconnections,

hardware, software, encryption techniques, transmissions, and network configuration. The SSP also provides an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements. In addition, the SSP delineates the responsibilities and expected behavior of all individuals who access the system. The SSP, typically written in conjunction with the Risk Assessment, is refined throughout the accreditation process.

A template for the SSP is provided in RMS. The template and the RMS Requirements Traceability Matrix (RTM) provide a basic structure to ensure consistency and completeness in the finished document. The DHS *Certification and Accreditation (C&A) Guidance for SBU Systems: Users Manual* provides detailed information on completing the SSP within RMS.

### 3.9.6 Contingency Plan

A Contingency Plan documents the management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster (see Section 3.5.3 for more information). The specific control requirements and level of effort are determined based on the IT system's security categorization. The level of resources for the Contingency Plan is based on the security categorization for the availability security objective:

- For systems with a **low impact for availability**, the system owner can determine the Contingency Plan format and content that is appropriate for the system and its environment. The Contingency Plan generated in RMS can also be used.
- For systems with a **moderate impact level for availability**, the default Contingency Plan template in RMS should be used.
- Systems with a **high impact level for availability** should develop a rigorous Contingency Plan. The DHS-developed high impact version of a contingency plan, *IT Contingency and Disaster Recovery Plan*, should be used. This template is found in the Additional Documents section of RMS. The high impact plan can be received in RMS when creating a package, by answering "Yes" to additional documents in the questionnaire. This template is also available in Attachment K to the 4300A Sensitive Systems Handbook.

The DHS *Certification and Accreditation (C&A) Guidance for SBU Systems: Users Manual* provides detailed information on developing the Contingency Plan within RMS.

### 3.9.7 Security Test and Evaluation (ST&E) Plan

The Security Test and Evaluation (ST&E) Plan outlines the plan, the process, and the procedures necessary to verify that the controls outlined in the SSP are in place and are operating as expected. The ST&E Plan template provided by RMS is the starting point for ensuring that there is a plan and methodology for testing and verifying that the management, operational, and technical controls are in place. The Requirements Traceability Matrix (RTM) generated by RMS when a C&A package is initiated is prepopulated with sample test procedures. However, the procedures will need to be tailored to the particular SSP, risks, and system environment, and they will need to be supplemented with detailed technical methods and procedures.

The complete ST&E Plan includes both the primary document as well as any supporting material. Typically, this material includes the documented test procedures contained with the RMS RTM by system

The DHS *Certification and Accreditation (C&A) Guidance for SBU Systems: Users Manual* provides detailed information on developing the ST&E Plan within RMS. Once the Risk Assessment, SSP, and ST&E Plan are completed and approved by the System Owner and agreed to with the Certifying Official, the ST&E testing can be conducted as part of the certification process. The test methods and procedures are documented as part of the ST&E Plan. Results of the testing are documented in the Security Assessment Report (see Section 3.9.9).

### **3.9.8 Contingency Plan Testing**

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

Contingency Plan testing is required only for systems with a moderate or high impact for the availability security objective; it is optional for systems with a low impact for availability. Testing requirements for systems with high, moderate, and low impact for availability are provided in Sections 3.9.8.1–3.9.8.3.

#### **3.9.8.1 Systems with High Impact Availability — *Testing required***

IT systems with high impact availability shall provide an established alternate site. If resources for establishing an alternate site are not available or identified, then a system shall not be categorized as high impact for availability.

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

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

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

### **3.9.8.2 Systems with Moderate Impact for Availability — *Testing required***

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

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

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

### **3.9.8.3 Systems with Low Impact for Availability — *Testing optional***

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

The DHS *Certification and Accreditation (C&A) Guidance for SBU Systems: Users Manual* provides detailed information on developing the ST&E Plan within RMS.

## **3.9.9 Security Assessment Report (SAR)**

The Security Assessment Report (SAR) summarizes the results of the ST&E and the system's compliance with the defined security controls in the SSP. The findings in the SAR can state that the system is fully compliant with the stated SSP and Risk Assessment or can state that the testing could not verify the claims in the SSP and Risk Assessment. If the testing finds that the system is compliant with the SSP and Risk Assessment, but residual risk still remains, the SAR must document what risk and actions will result. The results of the ST&E (updated RTM) are attached to support the findings in the SAR.

A SAR template is available in RMS. The DHS *Certification and Accreditation (C&A) Guidance for SBU Systems: Users Manual* provides detailed information on developing the SAR within RMS.

### 3.9.10 Authorization to Operate (ATO) Letter

The Authorization to Operate (ATO) letter or Denial to Operate letter is generated based upon the decision of the Designated Accrediting Authority (DAA). The DAA is given the accreditation package to review. The minimum acceptable package contains the following documents:

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

For operational systems, the DAA makes a risk-based decision either to grant full authorization to operate or deny authorization to operate. For development testing or for prototype systems, the DAA may grant an interim authorization to operate (IATO). An interim authorization provides a limited authorization to operate the IT system under specified terms and conditions and acknowledges greater risk to the organization's operations and assets for a limited period of time. A system undergoing development testing or a prototype system is *not* considered accredited during the period of limited authorization to operate.

Subsequent to the Key Decision Point 3 of the life cycle development and/or prior to allowing a system to become operational, the DAA must sign a formal ATO letter accrediting the system for operation in the DHS environment.

Decision	Criteria
Full Authorization to Operate (ATO)	After assessing the results of the security certification, if the Designated Accrediting Authority (DAA) accepts the residual risk to the agency's operations or assets, a full authorization to operate is issued for the IT system. The information system is accredited without any significant restrictions or limitations on its operation.
Interim Authorization to Operate (IATO) (for systems in development testing and prototype systems only)	After assessing the results of the security certification, the Designated Accrediting Authority may issue an interim authorization to operate (IATO) for systems in development testing and prototype systems. The IATO authorizes operation of the information system for up to 6 months. During this period, the effectiveness of security controls must be closely monitored. If the DAA has not officially accredited the testing or prototype system by the end of the IATO, the DAA may grant a second and final IATO for a period of up to 6 months. The

Decision	Criteria
	information system must be fully accredited by the end of the second IATO in order for it to receive a full ATO and become operational.
Denial of Authorization to Operate	After assessing the results of the security certification, if the DAA finds that the residual risk to the agency's operations or assets is unacceptable, the authorization to operate the IT system is denied. The IT system is not accredited and should not be placed into operation. For an IT system currently in operation, all activity should be halted.

The Plan of Action and Milestones (POA&M) is another part of the accreditation package. Weaknesses that will be accepted and not mitigated are documented in the final SAR and agreed to by the DAA prior to operation. Any weakness that is to be mitigated as part of the accreditation process must be documented in a Plan of Action and Milestones (POA&M). The POA&M documents the weaknesses of a system and the corrective actions that must be taken to address those weaknesses. The POA&M serves as a management tool for addressing and resolving security-related weaknesses. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates. For detailed guidance on the DHS POA&M process, consult the POA&M Process Guide (Attachment H to the DHS 4300A Sensitive Systems Handbook), or contact the DHS Compliance Help Desk (1-877-695-6955).

The DAA reviews the package and the Certifying Official's recommendation. In accrediting a system, the DAA can stipulate conditions on the accreditation (e.g., certain POA&M activities may need to be completed within a specific timeframe, or additional compensating controls may need to be implemented). The DAA writes the ATO letter (including any conditions) or Denial to Operate letter, signs the letter, and forwards it to the Certifying Official and System Owner.

The DHS *Certification and Accreditation (C&A) Guidance for SBU Systems: Users Manual* provides detailed information on the accreditation phase and on the ATO letter.

### 3.9.11 Annual Self-Assessments

NIST SP 800-26, *Security Self-Assessment Guide for IT Systems*, provides the IT security requirements that the DHS IT Security Program must satisfy for the FISMA annual review requirements. NIST SP 800-26 directs the use of an extensive questionnaire to determine whether the objectives of security controls installed in unclassified systems are being met. These guidelines are most often employed for identifying weaknesses or areas of needed improvement.

For FY 2007 and beyond, FIPS 200/NIST SP 800-53 must be used for the specification of security controls, and NIST SP 800-53A must be used for the assessment of security control effectiveness and for the annual FISMA reporting.

The annual assessments are performed within the Continuous Monitoring Phase of the accreditation, the purpose of which is to provide ongoing oversight and monitoring of the security controls in the IT system and to inform the authorizing official or designated representative when changes occur that may impact the security of the system. During this phase, the status of the IT system is monitored to ensure that residual risk is kept within an

acceptable level, and any significant changes to the system configuration or to the operational/threat environment that might affect system security are identified. DHS Components must re-accredit their IT systems every 3 years or whenever a major change occurs, whichever occurs first.

TAF addresses the annual self-assessments.

### 3.10 IT Security Review and Assistance

Note: This section is undergoing modification to incorporate policies and guidance relating to Component compliance reviews and site assistance visits.

The Federal Information Security Management Act of 2002 (FISMA) requires that a thorough review of the DHS IT Security Program be conducted on an annual basis. This review must include a report on the degree to which security requirements have been implemented, significant deficiencies discovered, remedial actions taken or in progress to correct deficiencies, and level of compliance with NIST standards. DHS 4300A Attachment E provides detailed information on FISMA reporting, including use of the automated COTS tool, Trusted Agent FISMA (TAF) (<https://tafisma.dhs.gov/>).

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

IT security review and assistance responsibilities are provided below.

<b>IT Security Review and Assistance Responsibilities</b>
<p><b>DHS CIO</b></p> <ul style="list-style-type: none"> <li>• Designates a full-time CISO.</li> <li>• Prepares the annual Congressional IT security compliance report as required by FISMA.</li> </ul> <p><b>CISO</b></p> <ul style="list-style-type: none"> <li>• Coordinates and prepares for the annual DHS Inspector General review of the IT Security Program.</li> <li>• Reviews and approves all DHS IT security policies.</li> <li>• Establishes and implements an IT Security Review and Assistance Program.</li> <li>• Prepares and distributes a review and assistance handbook based on applicable NIST guidance.</li> </ul> <p><b>DHS Compliance and Oversight Program Director</b></p>

<b>IT Security Review and Assistance Responsibilities</b>
<ul style="list-style-type: none"> <li>• Develops and implements a compliance review and assistance program.</li> </ul> <p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Implement an IT Security Review and Assistance Program at the Component level.</li> <li>• Schedule IT security review and assistance visits and ensure these visits are completed.</li> <li>• Provide trained personnel to participate in review and assistance visits.</li> <li>• Coordinate with ISSOs and provide guidance and oversight in identifying and documenting deficiencies and prioritizing them based on missions, risk, and funding.</li> <li>• Review and monitor Plans of Actions and Milestones (POA&amp;Ms).</li> <li>• Ensure POA&amp;M updates to the Trusted Agent FISMA database are timely (i.e., by March 10, June 10, September 15, and December 10 annually)</li> <li>• Coordinate issues with the Compliance and Oversight Program Director.</li> <li>• Generate candidate IT security policies, as the need arises, for CISO review and approval.</li> <li>• Review NIST and other directives for applicability to the DHS IT Security Program.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Prepare security self-assessment documentation as directed by the ISSM.</li> <li>• Identify personnel qualified to participate in review and assistance visits.</li> </ul> <p><b>System Owners</b></p> <ul style="list-style-type: none"> <li>• Ensure that ISSOs have access to resources adequate for conducting self-assessments and review and assistance visits.</li> <li>• Implement corrective actions for deficiencies found during self-assessments.</li> </ul> <p><b>Site Managers</b></p> <ul style="list-style-type: none"> <li>• Ensure that adequate personnel resources are available to participate in site assistance visits.</li> </ul>

### **3.10.1 Review and Assistance Management and Oversight**

The scope and complexity of the requirements necessary for the implementation and management of a successful IT security program requires active participation and oversight by a senior DHS official with a staff of qualified security professionals. In the DHS, the senior security manager is the CISO. This individual is appointed in writing by the DHS CIO, reviews and approves policy for the IT Security Program, oversees the DHS IT security assistance program, and prepares the annual assessment report.

### **3.10.2 IT Security Assistance**

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

### 3.10.3 IT Security Reviews

NIST SP 800-26, *Security Self-Assessment Guide for IT Systems*, has served as the basis for reviewing and evaluating the DHS IT Security Program and has helped satisfy the FISMA program review requirements. For FY 2007 and beyond, FIPS 200/NIST SP 800-53 will be used for the specification of security controls, and NIST SP 800-53A will be used for the assessment of security control effectiveness and for the annual FISMA reporting. System and site ISSOs have primary responsibility for completing the annual review and reporting results to senior management in accordance with the procedures established by the ISSM. The ISSM monitors ISSO performance, provides updates to the Trusted Agent FISMA database, and interacts with the DHS Compliance and Oversight Program Director.

### 3.11 Security Working Groups and Forums

Working groups and other forums representing various functional areas convene on a regular basis. Once the DHS IT security organization has been formalized and staffed, various working groups and forums such as those listed below will be established:

- DHS Information Systems Security Board
- DHS IT Security Training Working Group
- DHS Wireless Security Working Group

DHS senior security management officials such as the CISO and ISSMs will utilize the experience offered by the organizations coming together to form the new Department to decide the composition and missions of security working groups, forums, and committees. At that time charters detailing the roles and responsibilities of these new groups will be prepared and specific requirements will be included in this handbook.

#### 3.11.1 DHS Information Systems Security Board

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

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

#### 3.11.2 DHS IT Security Training Working Group

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

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

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

### 3.11.3 DHS Wireless Security Working Group (WSWG)

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

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

### 3.12 IT Security Policy Violation and Disciplinary Action

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

An IT security violation may result in disclosure of sensitive information to unauthorized individuals or in unauthorized modification or destruction of system data, loss of computer system processing capability, or loss or theft of any computer system resources. IT security violations also include a failure to adhere to DHS policy with respect to inappropriate use of the Departmental computer resources. The DHS CSIRC is normally responsible for initiating any disciplinary action following investigation of a security event by notifying appropriate law enforcement authorities, who pursue the investigation and recommend disciplinary action, if required.

<b>DHS Policy</b>
<b>a.</b> IT security-related violations are addressed in the <i>Standards of Ethical Conduct for Employees of the Executive Branch</i> and DHS employees may be subject to disciplinary action for failure to comply with DHS security policy, whether or not the failure results in criminal prosecution.

<b>DHS Policy</b>
<b>b.</b> Non-DHS Federal employees or contractors who fail to comply with Department security policies are subject to having their access to DHS IT systems and facilities terminated, whether or not the failure results in criminal prosecution.
<b>c.</b> Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions.

IT security policy violation and disciplinary action responsibilities are provided below.

<b>IT Security Policy Violation and Disciplinary Action Responsibilities</b>
<b>Users</b>
<ul style="list-style-type: none"> <li>• Be aware of IT security policies described in the handbook and in other references provided by DHS security officials.</li> <li>• Be aware of and understand the disciplinary actions associated with violations of IT security policy.</li> </ul>

### 3.13 Required Reporting

The Federal Information Security Management Act (FISMA) requires that the status of the DHS IT Security Program be reported to the Office of Management and Budget on a recurring basis. Quarterly reports and an annual summary report are submitted by the DHS Office of the CISO, Office of Information Security (OIS) to OMB. Using the Trusted Agent FISMA automated tool, Components update status information on a continual basis. This data is collected by OIS and compiled for the FISMA report and for other status reports. See DHS 4300A Attachment E for information on FISMA Reporting and DHS 4300A Attachment H for the POA&M Process Guide.

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

Note: Components shall utilize the Trusted Agent FISMA (TAF) product when reporting IT security program status information to the OIS.

FISMA reporting responsibilities are provided below.

<b>FISMA Reporting Responsibilities</b>
<p><b>ISSO/ISSM</b></p> <ul style="list-style-type: none"> <li>• Ensure that the TAF automated tool is utilized for required reporting.</li> <li>• Ensure that C&amp;A artifacts (e.g., Privacy Impact Assessment, System Security Plan, Security Test &amp; Evaluation Report, Contingency Plan Test Results, Risk Assessment, ATO letter) are uploaded into TAF.</li> </ul>

### 3.14 Privacy and Data Security

The DHS Privacy Office is responsible for privacy compliance across the Department, including assuring that technologies used by the Department sustain and do not erode privacy protections relating to the use of personal and Department information. The DHS Chief Privacy Officer has exclusive jurisdiction over the development of policy relating to personally identifiable information (PII). Questions concerning privacy-related policy should be directed to the DHS Privacy Office ([privacy@dhs.gov](mailto:privacy@dhs.gov); 571-227-3813). Please refer to the DHS Chief Privacy Officer web page for additional information.

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

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

For systems that perform electronic transactions, e-authentication requirements may apply.

#### 3.14.1 Personally Identifiable Information

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

General policies relating to personally identifiable information are provided below. Additional PII-related policies are included in the following sections:

- Section 3.9: Certification and Accreditation, Remediation, and Reporting. For systems involving personally identifiable information, the confidentiality security objective shall be assigned an impact level of at least moderate.

- Section 4.8.2: Laptop Computers and Other Mobile Computing Devices. All information stored on any laptop computer or other mobile computing device is to be encrypted.
- Section 5.2.2: Automatic Session Lockout. Sessions on workstations and on laptop computers and other mobile computing devices are to be terminated after 20 minutes of inactivity.
- Section 5.3: Auditing. Policies on audit logs of computer-readable extracts of personally identifiable information from databases and on erasure of these extracts are provided.
- Section 5.4.1: Remote Access and Dial-in. Remote access of personally identifiable information must be approved by the DAA. Strong authentication via virtual private network (VPN) or equivalent encryption (e.g., https) and two-factor authentication is required. Restrictions are placed on the downloading and remote storage of personally identifiable information accessed remotely.

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

### 3.14.2 Privacy Impact Assessments

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

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

Privacy impact assessment responsibilities are provided below.

<b>Privacy Impact Assessment Responsibilities</b>
<p><b>Privacy Officer</b></p> <ul style="list-style-type: none"> <li>• Determine and document privacy requirements. Review and approve the Privacy Threshold Analysis Template/PIA to determine if the document is adequate for DHS Privacy Office purposes.</li> </ul> <p><b>System Owner</b></p> <ul style="list-style-type: none"> <li>• Determine and document privacy requirements. Ensure the correct information is populated into the Privacy Threshold Analysis Template/PIA and uploaded to TAF for validation by the DHS Privacy</li> </ul>

<b>Privacy Impact Assessment Responsibilities</b>
<p>Office.</p> <p><b>C&amp;A Support Team</b></p> <ul style="list-style-type: none"> <li>• Complete the Privacy Threshold Analysis Template/PIA based upon information provided by the System Owner.</li> </ul>

### 3.14.3 Privacy Incident Reporting

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

<b>DHS Policy</b>
<p><b>a.</b> Any Component discovering a suspected or confirmed incident must coordinate with the Component Privacy Office or PPOC and ISSM in order to evaluate and subsequently report the incident to the DHS SOC.</p>
<p><b>b.</b> The Component Privacy Officer or PPOC, in cooperation with the ISSM, shall jointly evaluate the incident, but the ISSM is responsible for reporting the incident to the Component CSIRC/SOC (or directly to the DHS CSIRC if the Component does not have its own SOC/CSIRC).</p>
<p><b>c.</b> The ISSM shall report ALL types of privacy incidents, whether or not they involve IT resources. This unitary reporting process shall remain in effect until each Component has a Privacy Office or PPOC who can fulfill the reporting duties.</p>
<p><b>d.</b> DHS personnel must also report suspected or confirmed privacy incidents or incidents involving PII to their Program Manager immediately upon discovery/detection, regardless of the manner in which it might have occurred.</p>

<b>Privacy Incident Reporting Responsibilities</b>
<p><b>DHS Personnel</b></p> <ul style="list-style-type: none"> <li>• Provides notification of incident to Program Manager</li> </ul>
<p><b>Program Manager</b></p> <ul style="list-style-type: none"> <li>• Prepares preliminary privacy incident report and passes report to the ISSM or Component CSIRC/SOC</li> </ul>
<p><b>ISSM/Component CSIRC/SOC</b></p> <ul style="list-style-type: none"> <li>• Evaluates Privacy Incident; Prepares and Submits Incident Report in SOC Online Incident Handling System</li> </ul>
<p><b>DHS SOC</b></p> <ul style="list-style-type: none"> <li>• Notifies CPO, CISO, CIO and Dep. CIO; Processes and Transmits Privacy Incident Report to US-CERT</li> </ul>

### 3.14.4 E-Authentication

To ensure that online Government services are secure and protect privacy, some type of identity verification or authentication (“e-authentication”) is needed. Each DHS IT system must be evaluated as to whether e-authentication requirements apply.

E-authentication guidance is provided in the following:

- OMB M-04-04: E-Authentication Guidance for Federal Agencies, December 16, 2003
- NIST SP 800-63: Electronic Authentication Guideline, April 2006

See Section 3.9.3 (E-Authentication) for additional information.

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

### 3.15 DHS Chief Financial Officer – Designated Financial Systems

DHS CFO designated financial systems are systems that require additional management accountability and effective internal control over financial reporting. This section provides additional requirements for these systems based on OMB Circular A-123, *Management’s Responsibility for Internal Control (A-123)* Appendix A. These requirements are in addition to the other security requirements established in this document and other CFO developed financial system Line of Business requirements. *Wherever there is a conflict between this and other sections of this policy regarding requirements for CFO designated financial systems, this section takes precedence.*

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

<b>DHS Policy</b>
<b>a.</b> System owners are responsible for ensuring that Security Test and Evaluation (ST&E) plans and security assessments of key security controls for CFO designated financial systems are completed

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

<b>DHS Policy</b>
change to CFO designated financial system identified in the DHS inventory.

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

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

Key controls are defined as a control, or a set of controls, which address the relevant assertions for a material activity or significant risk. Key controls are required to be identified in system security plan and tested as part of an annual ST&E. System owners may perform rolling compliance tests that test other (non-key) controls annually and controls that were not tested in the previous years. Documentation and testing artifacts (see Table 3) for CFO designated financial systems will be tracked and captured through the DHS information assurance (IA) compliance systems. These requirements must be met within the specified timeframes. Failure to do so will result in the suspension of the systems' ATO.

Table 3: Documentation and Testing Artifacts

<b>Artifact</b>	<b>Required Action</b>	<b>Frequency</b>	<b>Completion Deadline</b>	<b>Reporting Requirements</b>
Risk Assessment (RA)	A complete RA shall be conducted	Annual	As determined by the ISSM	Report no later than (NLT) Sep 30 of each year
System Security Plan (SSP)	The SSP shall be evaluated and updated	Annual	During first quarter of each FY	Report NLT Sep 30 of each year
Key Security Controls Security Assessment Results	Key security controls shall be evaluated and updated	Annual	During first quarter of each FY	Report completion NLT Dec 31 of each year
Disaster Recovery (DR) Plan Results	The DR plan shall be exercised	Annual	First quarter of each FY	Report completion NLT Dec 31 of each year

<b>Artifact</b>	<b>Required Action</b>	<b>Frequency</b>	<b>Completion Deadline</b>	<b>Reporting Requirements</b>
Vulnerability Assessment (VA)	A complete VA shall be conducted	Semi-Annual	One assessment completed during the first quarter of each FY; Second assessment completed during the third quarter.	Report completion of one assessment NLT Dec 31; report completion of second assessment NLT Jun 30
Critical Patch Installation	Installation of critical patches shall be verified	Semi-Annual	As determined by the ISSM	Report NLT Sep 30 of each year

## **4.0 OPERATIONAL CONTROLS**

Operational Controls address security methods focusing on the mechanisms primarily implemented and executed by people. These controls are placed to improve the security of a group, a particular system, or a group of systems. These controls require technical or specialized expertise and rely on management and technical controls.

### **4.1 Personnel**

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

#### **4.1.1 Citizenship, Personnel Screening, and Position Categorization**

DHS policy requires that only Government and contractor personnel who are U.S. citizens shall be granted access to DHS systems processing sensitive information. However, at times there is a need to grant access to non-U.S. citizens. The Component Head or designee may grant access to DHS systems for non-DHS Government employees and/or non-U.S. citizens only when (1) the individual is a legal permanent resident of the United States or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State, (2) all required security forms specified by the Government and any necessary background check have been satisfactorily completed, (3) a compelling reason exists for using this individual instead of a U.S. citizen, (4) the exception to the U.S. citizenship requirement is in the best interest of the U.S. Government, and (5) the DHS Chief Security Officer and the Chief Information Officer or their designees concur in approving access for the individual. DHS 4300A Attachment J provides an electronic form for requesting an exception to the U.S. citizenship requirement.

All personnel accessing DHS systems are required to have an appropriate security clearance and a valid need to know in order to access these systems. All DHS employees must have favorably adjudicated background investigations commensurate with the defined sensitivity level of the positions they hold. Determining the appropriate position sensitivity level is based on such factors as the type and degree of harm (e.g., disclosure of sensitive information, interruption of critical processing, computer fraud) the individual can cause through misuse of the computer system.

Another prudent safeguard is to ensure that individuals who support DHS systems are highly qualified technically and are adequately trained for the position they occupy. This can reduce the risk of unintentional actions. A major threat to an IT system can be the loss of key technical personnel. While unintentional acts and accidents cannot be eliminated, effective training can help to mitigate the possibility or frequency of unintentional user errors.

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

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

Responsibilities related to personnel issues are provided below.

<b>Citizenship, Position Categorization, and Personnel Screening Responsibilities</b>
<p><b>Component Head</b></p> <ul style="list-style-type: none"> <li>• Requests exceptions to the DHS requirement for U.S. citizenship for non-U.S. citizens who require access to DHS systems processing sensitive information.</li> </ul> <p><b>System Owners</b></p> <ul style="list-style-type: none"> <li>• Designate the position sensitivity level for all in-house or contractor positions that use, develop, or operate IT systems.</li> </ul> <p><b>Security Managers</b></p> <ul style="list-style-type: none"> <li>• Ensure all personnel who use, develop, or operate DHS IT systems have a favorably adjudicated background investigation commensurate with the defined sensitivity level associated with their position.</li> </ul>

#### **4.1.1.1 Background Investigations for Government Employees**

DHS employees will undergo the appropriate security investigations to obtain the needed clearances for their positions. The types of security investigations—from DHS MD 11050.2, Personnel Security Program—are summarized below. These are listed generally from least to most comprehensive.

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

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

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

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

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

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

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

#### **4.1.1.2 Background Investigations for Contractor Personnel**

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

RISK LEVEL	SECURITY FORMS REQUIRED	TYPE OF INVESTIGATION REQUIRED		PRELIMINARY CHECKS REQUIRED FOR EOD / WAIVER DETERMINATION	
		IT-Computer Positions	Non-IT Computer Positions	IT Positions (waiver NTE 100 days)	Non-IT Positions
HIGH	<ul style="list-style-type: none"> <li>– SF 85P</li> <li>– FD 258</li> <li>– Credit Release Form</li> </ul>	BI	LBI	Favorable review of forms Favorable NAC Scheduling of the BI**	Favorable review of forms Favorable NAC Submission of the LBI
MODERATE	<ul style="list-style-type: none"> <li>– Non-Disclosure Statement</li> <li>– SF 85P-S*</li> </ul>	MBI	NACIC	Favorable review of forms Favorable NAC Scheduling of the MBI	Favorable review of forms Favorable NAC + credit check
LOW	<ul style="list-style-type: none"> <li>– SF-85P</li> <li>– FD-258</li> </ul>	N/A	Favorable review of forms FP and name check	N/A	

\* Only Weapons-Carrying Contract Guards must complete the SF 85P-S in addition to SF 85P

\*\* Eligible for access only to the moderate risk level.

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

#### 4.1.2 Rules of Behavior

Rules of behavior regarding the access of DHS systems and the use of its IT resources are a vital part of the DHS IT Security Program. Rules of behavior that are understood and followed help ensure the security of systems and the confidentiality, integrity, and availability of sensitive information. Rules of behavior inform users of their responsibilities and let them know they will be held accountable for their actions while they are accessing DHS systems and using DHS IT resources that are capable of accessing, storing, receiving, or transmitting sensitive information. The DHS rules of behavior apply to DHS employees and to DHS support contractors.

DHS Policy
<p><b>a.</b> Components shall define rules of behavior for all IT systems and ensure that users are trained regarding these rules and are aware of the disciplinary actions that may result from violating these rules.</p>

<b>DHS Policy</b>
-------------------

<p><b>b.</b> Users shall sign rules of behavior prior to being granted IT accounts or access to any DHS IT systems or data.</p>
---

Rules of behavior responsibilities are provided below.

<b>Rules of Behavior Responsibilities</b>
---

<p><b>System Owners</b></p> <ul style="list-style-type: none"> <li>• Develop and enforce rules of behavior for IT systems under their authority.</li> </ul>
---

<p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Advise system owners concerning the establishment and implementation of a set of rules of behavior for DHS IT systems.</li> <li>• Ensure that rules of behavior for DHS general support systems and major applications are included in the Security Plan.</li> <li>• Ensure users read and sign general rules of behavior regarding use of DHS systems and IT resources and rules of behavior specific to the DHS systems to which they will be given access.</li> </ul>
---

<p><b>Users</b></p> <ul style="list-style-type: none"> <li>• Adhere to the general rules of behavior regarding the use of DHS systems and IT resources and to the system-specific rules of behavior for the IT systems to which they have been granted access.</li> </ul>
---

Rules of behavior must be developed for each automated information system and general support system. These rules must clearly delineate responsibilities and the expected behavior of all individuals with access to the system. As such, they form the basis for security awareness and training. The rules must state the consequences of inconsistent behavior or noncompliance. Rules of behavior must be in writing and must be made available for each user to read and sign before that user is granted access to the system.

DHS 4300A Attachment G provides guidance for developing system-specific rules of behavior and guidance for developing general rules of behavior that apply to all DHS systems and IT devices that are capable of accessing, storing, receiving, or transmitting sensitive information.

Any person who is in noncompliance with the rules of behavior is subject to penalties and sanctions, including verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, criminal or civil prosecution, or termination, depending on the severity of the violation.

#### **4.1.3 Access to Sensitive Information**

Sensitive information is information that if lost, misused, or accessed or modified without authorization could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act could be adversely affected.

To protect sensitive information and limit the damage that can result from accident, error, or unauthorized use, the principle of least privilege must be applied. The principle of least privilege requires that users be granted the most restrictive set of privileges (or lowest clearance)

needed for performance of authorized tasks—i.e., users should be able to access only the system resources needed to fulfill their job responsibilities.

**Principle of Least Privilege:** Requires that a user be granted the most restrictive set of privileges (or lowest clearance) needed for performance of authorized tasks.

Application of this principle ensures that access to sensitive information is granted only to those users with a valid need to know.

#### DHS Policy

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

Access to sensitive information responsibilities are provided below.

#### Access to Sensitive Information Responsibilities

##### System Owners

- Ensure users have a valid *need to know* prior to granting access to information contained in DHS IT systems.
- Ensure users have the appropriate level of clearance prior to being granted access to sensitive IT resources.

##### ISSOs/System Administrators

- Ensure users have a valid requirement prior to being granted access to DHS IT systems.
- Ensure users have the appropriate level of clearance prior to being granted access to sensitive IT resources.

Section 5.2, *Access Control*, provides implementation guidelines regarding access to sensitive information.

#### 4.1.4 Separation of Duties

Separation of duties (required by OMB Circular A-130) mandates the assignment of portions of security-related tasks to several individuals. This separation is necessary for adequate internal control of sensitive IT systems. This also ensures that no single individual has total control of the system's security mechanisms and prevents a single individual acting alone from subverting a critical process or otherwise completely compromising the system.

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

#### DHS Policy

Components shall divide and separate duties and responsibilities of critical IT system functions among different individuals to minimize the possibility that any one individual would have the necessary authority or systems access to be able to engage in fraudulent or criminal activity.

Responsibilities related to separation of duties are provided below.

<b>Separation of Duties Responsibilities</b>
<p><b>System Owners</b></p> <ul style="list-style-type: none"> <li>• Ensure personnel work assignments comply with DHS policy regarding separation of duties for sensitive IT systems.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure controls are in place that enforce compliance with DHS policy in regards to separation of duties.</li> </ul>

Assignment and segregation of system responsibilities must be clearly defined and documented for all DHS IT systems. Segregation of responsibilities, in addition to appropriate access controls, is intended to ensure that no individual has all necessary authority or information access to be able to engage in fraudulent activity without collusion. For this reason, it is essential that thorough and specific job descriptions be documented for every individual working with DHS IT systems and sensitive information.

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

Whenever practical, the positions of security administrator and system administrator need to be filled by separate individuals. The same principle should also be applied to ISSO and system administrator positions. When having separate system and security administrators is not possible, the system administrator will be responsible for maintaining the system security configuration of systems, but will be subject to periodic audit/configuration review by the ISSO.

Note: If a Component does not have sufficient manpower resources necessary to meet strict separation of duties requirements, the appropriate DAA may authorize exceptions provided that a shortage of personnel is formally identified as a residual risk.

#### **4.1.5 IT Security Awareness, Training, and Education**

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

5 CFR part 930, subpart C, as revised, requires that all users (Federal employees as well as contractors) of Federal information systems must be exposed to security awareness materials at least annually. Additional to the annual training requirement, training will occur when employees are hired (they must receive the training before they are allowed access to systems), when system security changes occur, when an employee's work responsibilities change."

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, requires that persons be trained in their responsibilities and in the "rules of behavior" for using general support systems (e.g., LANs) and for using major applications before being given access to those systems or applications. Computer security training must be addressed in the security

plan for each IT system. In addition, Component ISSMs shall prepare and submit to the DHS IT Security Training Program Director a training plan outlining their plans for IT security awareness, training, and education for the year. The plans shall follow the guidance in the DHS Component Information Technology (IT) Security Awareness, Training and Education Plan template, issued by the DHS IT Security Training Office.

In 5 CFR Part 930, the Office of Personnel Management (OPM) requires Federal agencies to identify employees responsible for the management or use of computer systems that process sensitive information and to provide training to the following groups: executives; program and functional managers; information resources management (IRM), security, and audit personnel; automated data processing (ADP) management and operations personnel; and end users. It requires that employees in these groups receive their required training within 60 days of their appointment. It also requires that additional training be provided whenever there is a significant change in the agency's IT security environment or procedures, or when an employee enters a new position involving the handling of sensitive information. It also requires that computer security refresher training be given as frequently as determined necessary by the agency based on the sensitivity of the information that the employee uses or processes.

The Federal Information Security Management Act of 2002 (FISMA) tasks the Chief Information Officer (or comparable official) of each agency with training and overseeing personnel with significant responsibilities for information security. Additionally, FISMA requires that each agency include security awareness training within an agency-wide information security program. The security awareness training must inform personnel, including contactors and other users of IT systems that support the operations and assets of the agency, of (1) information security risks associated with their activities and (2) their responsibilities in complying with agency policies and procedures so that such risks will be reduced. FISMA also requires each agency to include as part of its performance plan a description of the resources—including budget, staffing, and training—that are necessary to implement the program.

NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, provides Federal agencies with detailed guidelines for developing a robust training program for staff within 26 security-related roles. This document will be used to the extent that it is practical in developing and implementing awareness and training materials and courses for DHS employees and support contractors.

<b>DHS Policy</b>
<b>a.</b> Components shall establish an appropriate IT Security Training Program for users of DHS systems.
<b>b.</b> DHS personnel and contractors accessing DHS IT systems shall receive initial training and annual refresher training in security awareness and accepted security practices.
<b>c.</b> DHS personnel and contractors with significant security responsibilities (e.g., ISSOs, system administrators) shall receive initial specialized training, and annual refresher training thereafter, specific to their security responsibilities prior to being granted access to DHS IT systems.
<b>d.</b> Components shall maintain training records, to include name and position, type of training received, and costs of training. IT awareness training must be completed before IT accounts are authorized.

<b>DHS Policy</b>
<p><b>e.</b> Unless a waiver is granted by the ISSM, user accounts and access privileges, including access to email, shall be disabled for those DHS employees who have not received annual refresher training.</p>
<p><b>f.</b> Components shall prepare and submit an annual training plan, outlining their plans for IT Security Awareness, Training and Education. This plan shall follow the guidance in the DHS Component Information Technology (IT) Security Awareness, Training and Education Plan template, issued by the DHS IT Security Training Office.</p>
<p><b>g.</b> Training plans shall include awareness of internal threats and basic IT security practices.</p>
<p><b>h.</b> Components shall prepare and submit IT security awareness, training, and education statistics to the DHS IT Security Training Program Director on a quarterly basis. These statistics shall include:</p> <ul style="list-style-type: none"> <li>– Total number of personnel and number of personnel that have received awareness training.</li> <li>– Total number of personnel with significant security responsibility and the number that have received role-based training.</li> <li>– The cost of any agency-provided IT security training or materials for the year.</li> </ul> <p>Components must also provide:</p> <ul style="list-style-type: none"> <li>– Brief descriptions of the awareness and training provided to personnel.</li> <li>– Information concerning how they have explained policies relating to Peer-to-Peer (P2P) file sharing to all system users.</li> </ul>
<p><b>i.</b> Components shall provide evidence of training by submitting copies of training schedules, training rosters, training reports, etc., upon request of the DHS IT Security Training Office, or during onsite validation visits performed on a periodic basis.</p>

IT security awareness, training, and education responsibilities are provided below.

<b>IT Security Awareness, Training, and Education Responsibilities</b>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Establish overall policy for IT security awareness, training, and education.</li> <li>• Provide guidance on preparing and attending security awareness and training sessions.</li> <li>• Submit to the DHS IT Security Training Program Director a training plan outlining their plan for IT Security Awareness, Training, and Education for the year.</li> <li>• Analyze, on a quarterly basis, security awareness and training statistics submitted by the ISSOs and COTRs and submit a summary of these statistics to the DHS IT Security Training Program Director.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that all new employees, including contractors, complete an initial Government- or contractor-sponsored security awareness course as part of their orientation.</li> <li>• Unless an ISSM waiver is issued, disable all accounts and access privileges, including access to email, of those DHS users who failed to complete the annual security refresher course.</li> </ul>

### **IT Security Awareness, Training, and Education Responsibilities**

- Ensure that all users, including all contractors, read and sign rules of behavior for the use of systems and applications prior to their being given access to those systems and applications.
- Implement annual awareness refreshers for employees and support contractors involved in the management, use, or operation of IT systems that process sensitive information.
- Maintain a record of security awareness and training that includes the name and position of the person trained, the type of training, the date of the training, and the cost of the training.
- Submit to the ISSM, on a quarterly basis, statistics on initial and refresher security awareness and training.
- Implement continued training for personnel when there is a significant change in the system security environment or in procedures, or when an employee enters a new position involving the handling of sensitive information.

#### **COTRs**

- Ensure that contractors have their personnel complete an initial security awareness course as part of their orientation.
- Ensure that contractors have their personnel complete a refresher awareness course each year.
- Ensure that contractors have their personnel sign rules of behavior for the use of systems and applications prior to their being given access to those systems and applications.
- Ensure that contractors provide additional security awareness training to their personnel whenever there is a significant change in the system security environment or in procedures, or when contractor personnel enter a new position.
- Ensure that contractors maintain a record of their personnel who have completed initial and refresher security awareness training, with the record to include the name of the person trained, the type and date of the training, and training cost.
- Ensure that contractor security awareness and training statistics are provided to the ISSM on a quarterly basis.

#### **4.1.5.1 Initial Awareness**

Components must give newly hired employees an initial IT security awareness course and have them read and sign a rules of behavior acknowledgement statement before giving those employees being given access to any DHS network resources or applications. The awareness course and the rules of behavior should be a part of the orientation process. Components must also provide an initial awareness course to newly hired contractor staff or ensure that the contractors provide an equivalent course for their staff. Participation in the awareness course is mandatory. Records of the training must be maintained and retained to verify compliance; records must include the employee's name and position, the type of training received, and the date of training.

Appropriate media for providing this initial awareness include seminars, presentations, awareness videotapes, and computer-based products delivered via CD-ROM, intranet/Internet, and/or LAN.

#### 4.1.5.2 Refresher Awareness

Components must provide an IT security awareness refresher course to employees annually; they must also either provide an annual awareness refresher course for contractor staff or ensure that contractors provide an equivalent refresher course for their staff. Participation in the refresher course is mandatory. User accounts and access privileges, including access to email, will be disabled for those who have not received annual refresher training. The appropriate ISSM may issue a waiver to this requirement. Records of the training must be maintained and retained to verify compliance; records must include the employee's name and position, the type of training received, and the date of training.

Appropriate media for providing refresher awareness include seminars, presentations, awareness videotapes, and computer-based products delivered via CD-ROM, intranet/Internet, and/or LAN.

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

#### 4.1.5.3 Ongoing Awareness Activities

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

#### 4.1.5.4 Role-Based Training

DHS personnel and contractors who have significant security responsibilities—e.g., ISSOs, network administrators, system administrators, and DAAs—must receive specialized training specific to their security responsibilities. Specialized security-related training must also be provided to senior managers, system owners, and IT Project Managers. Components must ensure that such personnel receive this specialized training annually. The level of training shall be commensurate with the individual's duties and responsibilities. Components must track, by name and position, the type of the training received, the dates of the training, and the costs of the training.

#### 4.1.6 Separation from Duty

This section addresses the procedures to be followed when an employee or contractor terminates employment or transfers to another organization.

<b>DHS Policy</b>
<p><b>a.</b> Components shall implement procedures to ensure that system accesses are revoked for employees or contractors who leave the Component or are reassigned to other duties. Accounts for personnel on extended absences shall be temporarily suspended.</p>
<p><b>b.</b> Components shall establish procedures to ensure that sensitive information stored on any media is transferred to an authorized individual upon termination or reassignment of an employee or contractor.</p>

Responsibilities related to separation from duty are provided below.

### Separation from Duty Responsibilities

#### **System Owners/Senior Site Managers**

- Implement procedures to ensure appropriate system access privileges are revoked for employees or contractors who either leave the Component or are reassigned to other duties.

#### **Supervisors**

- Notify system administrators in writing when employees or contractors no longer require access to DHS IT systems.
- Retrieve all sensitive data from departing employees and contractors.

#### **Network/System Administrators**

- Disable or delete user accounts when notified that an individual's access to DHS IT systems is reassigned or terminated.

#### **Site Security Officers**

- Change combinations to all locks and safes when an employee or contractor with access has been reassigned or terminated.
- Collect all keys, badges, and other devices used to gain access to premises, information, or equipment from employees and contractors who have been terminated or reassigned.

#### **Employees and Contractors**

- Turn in laptops, cell phones, PEDs, secure ID tokens, and other Government-owned devices to the local property administrator in accordance with local procedures when reassigned or terminated.

In most circumstances, the transfer or termination of an employee or contractor is amicable. Allowing an employee or contractor to complete his or her duties and obligations through the last day of employment is normally the most effective course of action.

When the employee or contractor demonstrates resentment because of termination of duties, it is often better to immediately eliminate the employee's contact with the organization, including system access. It is also recommended that the employee be escorted from the premises, and that personal items be mailed or delivered at a later date. The security office for each DHS site should assist in creating a prudent plan of action.

DHS Components are to adhere to the following guidelines when dealing with employee separation or termination:

- **Revoke all authorizations.** All authorizations granted to a departing employee or contractor are to be revoked. When an employee leaves the DHS, personnel paperwork for resignation or transfer to another Government agency is processed in the personnel and payroll system. LAN access and other client/server systems must be revoked. It is the responsibility of the supervisor or IT Project Manager to ensure that these steps have been followed and the necessary levels of access have been revoked. If the departing employee or contractor authorizations include the granting of authorization to others, this must be reviewed and changed accordingly. If a user is being transferred within the DHS, it is possible to transfer the employee's user ID. However, since users are given access on a need-to-know basis, the supervisor must request that the user's access privileges be deleted before transferring. The proper level of access will be granted once the employee is officially in the new position.

- **Retrieve hard and soft copy sensitive information.** The supervisor should collect all hard and soft copy sensitive information.
- **Retrieve all keys, badges, and other access devices.** The local ISSO in coordination with the site security officer should collect all keys, badges, and other devices used to gain access to premises, information, or equipment.
- **Change locks.** The security officer will assist in changing combinations of all locks and safes known to the departing employee or contractor immediately.
- **Turn in Government-owned equipment.** Employees and contractors must turn in laptops, cell phones, portable electronic devices (PED), secure ID tokens, and other Government-owned property to the local property administrator in accordance with local procedures, and provide evidence at their exit interview that this action has been accomplished.
- **Conduct exit interview.** All employees and contractors leaving their positions must participate in an exit interview. One purpose of an exit interview is to provide management with information as to why people are leaving. This information will permit management to make positive changes, if necessary. The employee should return all DHS sensitive materials, and receive information concerning restrictions on divulging certain DHS information. There should be a review of any special conditions to the departing employee or contractor employment, such as the denial of right to use certain information. The exit meetings should occur prior to an employee or contractor departure from the DHS. Failure to complete this step may make subsequent legal recourse (if needed) more difficult or impossible. The cognizant personnel or security office should conduct the exit interview in accordance with local procedures.

## 4.2 IT Physical Security

DHS security personnel must address physical security as an integral element in the effective implementation of an IT security program. Physical security represents the “first line of defense” against intruders and adversaries attempting to gain access to DHS facilities and IT systems. Like other aspects of information assurance, physical security technology is advancing rapidly. Though the “moat around the castle” approach was once a sufficient means of deterrence, intruders are now far more sophisticated.

Physical security must be addressed during each step of the risk management cycle. Physical security vulnerabilities are identified during the risk assessment. Cost-effective controls are then documented in the security plan. These controls are then evaluated during the Security Test and Evaluation (ST&E). Any residual risks must be documented in the C&A package and reviewed on an annual basis. IT systems must be physically and environmentally protected to prevent unauthorized disclosure, denial of service, destruction, or modification.

Section 4.2.1, General Physical Access, provides general physical security guidance for sensitive systems. Section 4.2.2, Sensitive Facility, addresses specific security considerations for facilities housing IT systems that store or process classified data.

### 4.2.1 General Physical Access

General physical access controls restrict the entry and exit of personnel from an area, such as an office building, data center, or room containing IT equipment. These controls protect against threats associated with the physical environment. It is important to review the effectiveness of general physical access controls in each area during business hours and at other times.

Effectiveness depends not only on the characteristics of the controls used but also on their implementation and operation.

<b>DHS Policy</b>
<b>a.</b> Access to DHS buildings, rooms, work areas, spaces, and structures housing IT systems, equipment, and data shall be limited to authorized personnel.
<b>b.</b> Controls for deterring, detecting, restricting, and regulating access to sensitive areas shall be in place and will be sufficient to safeguard against possible loss, theft, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters.
<b>c.</b> Controls shall be based on the level of classification and risk, determined in accordance with Departmental security policy.
<b>d.</b> Visitors must sign in upon entering DHS facilities, be escorted during their stay, and sign out upon leaving. Non-DHS contractors' access shall be limited to those work areas requiring their presence. Visitor logs shall be maintained and available for review for one year.
<b>e.</b> These requirements will extend to DHS assets, located at non-DHS facilities or non-DHS assets and equipment hosting DHS data.

General physical access responsibilities are provided below.

<b>General Physical Access Responsibilities</b>
<p><b>Facility Managers</b></p> <ul style="list-style-type: none"> <li>• Ensure that physical controls are in place.</li> <li>• Ensure that environmental controls are in place.</li> <li>• Ensure that physical and environmental controls are in working order at all times.</li> <li>• Ensure that access control logs are maintained and reviewed for the facility and all computer rooms.</li> </ul> <p><b>Site Security Officers/ISSOs</b></p> <ul style="list-style-type: none"> <li>• Provide specific security briefings to DHS employees and contractors, as necessary.</li> <li>• Assess the adequacy of physical security controls as part of the risk management cycle.</li> <li>• Change combinations to locks on security containers housing sensitive information, funds, and other valuables that must be safeguarded.</li> <li>• Conduct periodic inspections of offices and areas under their jurisdiction, during or after working hours, to ensure sensitive and proprietary materials are being adequately safeguarded.</li> <li>• Ensure security violations are appropriately reported and investigated, in accordance with DHS requirements.</li> <li>• Provide oversight of the issuance and return of Service badges, credentials, and identification documents; ensure proper reporting of the loss or theft of Service badges, credentials and identification documents.</li> </ul>

<b>General Physical Access Responsibilities</b>
<ul style="list-style-type: none"> <li>• Apply the security disciplines to the contractor environment.</li> <li>• Ensure Government-owned and controlled property, funds, and valuables are properly safeguarded and accounted for.</li> <li>• Ensure the physical security of IT Systems within their jurisdiction.</li> <li>• Ensure that physical and environmental security controls are addressed in the Security Plan.</li> <li>• Address physical security as an integral part of the risk management process.</li> <li>• Ensure that physical security risks are reviewed and evaluated throughout the SDLC.</li> </ul> <p><b>Users</b></p> <ul style="list-style-type: none"> <li>• Adhere to established security policies.</li> <li>• Display building passes or other ID when required.</li> <li>• Challenge individuals who are not in compliance with established requirements.</li> <li>• Ensure that uncleared visitors are escorted at all times.</li> </ul>






#### 4.2.1.1 Physical Controls

Physical security encompasses the full range of protective measures designed to safeguard personnel and prevent unauthorized access to, and the loss, theft, destruction, sabotage, or compromise of equipment, facilities, material, and information. Physical controls include barriers, badges, guard or security forces, supporting infrastructure, contingency and emergency support, lighting, facility intrusion detection systems, and surveillance systems. Physical security protects computer facilities as well as individual computer systems and personnel. Standards for physical security must be based on an analysis of mission criticality, severity of impact levels, local criminal and intelligence threats, and the value of the telecommunications and automated information systems equipment contained within the facility being protected as well as the value of the data being processed.

Security personnel must ensure that physical security controls are considered throughout the life of the system. At a minimum, they should be reviewed in conjunction with the annual self-assessments and during each C&A cycle. The following in-place and planned controls associated with the following physical security features should be included in the appropriate security plan:

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

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

Normally, not all of the above security features will be necessary for every facility. ISSOs and site security officers must determine, based on the criticality of the systems and sensitivity of the data being processed, which security features are warranted.

#### **4.2.1.2 Building Passes**

Building passes must be issued and displayed by direct hire and contract employees at all facilities that store or process sensitive information.

Building passes should be displayed above the waist and below the neck with the photo side facing out. Each visitor must be issued a temporary building pass, which must be turned in before the visitor exits the facility.

Any persons not displaying proper credentials should be challenged. If there is any doubt as to their authorization, they are to be escorted from the area and local security personnel are to be contacted. Security personnel and supervisors at all management levels must ensure that all DHS staff, including contractors, are made aware of this requirement through awareness sessions and other means. Supervisors are expected to periodically reinforce this requirement during staff meetings and through emails and other communication methods. Where practical, challenge procedures should be posted.

#### **4.2.1.3 Property Removal**

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

#### **4.2.1.4 Loss or Theft of Property**

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

#### **4.2.1.5 Environmental Controls**

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

- Fire protection, detection, and suppression
- Water damage risk reduction, detection, and corrective measures, and devices for water hazard prevention
- Electronic power supply protection, to include uninterruptible power supplies for multiuse systems and surge protectors for stand-alone systems

- Temperature and humidity recording, monitoring, and alert systems (e.g., humidograph)
- Housekeeping protection from dirt and dust
- Combustible cleaning supplies protection (not to be kept in computer areas)
- Appropriate personnel safety features (evacuation routes specified)
- Emergency exit provisions, such as equipping emergency and exit-only doors with hardware that permits immediate egress in the event of an emergency

#### **4.2.1.6 Fire Protection**

Fire protection systems should be serviced by professionals on a recurring basis to ensure the system stays in proper working order. The following should be taken into consideration when developing a fire protection strategy:

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

#### **4.2.1.7 Electronic Power Supply Protection**

Electrical power must be filtered through an uninterruptible power supply (UPS) system for all servers and critical workstations. A surge suppressing power strip is necessary for all other ADP equipment to protect it from sudden power surges. For larger and more critical systems it may be appropriate to have an electrical generator available for the most critical of operational requirements.

#### **4.2.1.8 Temperature and Humidity Control**

The condition of the air is important to prevent damage to IT equipment. The following should be considered when developing a strategy for temperature and humidity control:

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

Check the system documentation for the proper levels for your hardware. Security personnel should obtain a device that will sound an alarm and send out an automatic notification (via email or pager) when the operating environment exceeds recommended boundaries.

#### 4.2.1.9 Housekeeping Considerations

Housekeeping is another important area to monitor.

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

#### 4.2.1.10 Personnel Safety Features

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

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

#### 4.2.1.11 Emergency Exits

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

### 4.2.2 Sensitive Facility

Facilities supporting large-scale IT operations, such as enterprise servers and telecommunications facilities, require consideration of additional environmental and physical controls as determined by a risk analysis.

Section 4.2.1 provides procedural guidance for both general physical access and sensitive facilities. For facilities supporting large-scale IT operations, all of the physical security features outlined in Section 4.2.1 must be addressed. The risk assessment shall specifically document the rationale for any such physical security controls not incorporated.

<b>DHS Policy</b>
<b>a.</b> Facilities processing, transmitting, or storing sensitive information shall incorporate physical protection measures based on the level of risk. The risk should be determined in accordance with Departmental security policy.
<b>b.</b> Any sensitive information or data not suitable for public dissemination shall be secured in one of the following: a locked office, room, desk, bookcase, file cabinet, or other storage prohibiting access by

DHS Policy
unauthorized persons.

See Section 4.2.1 for a summary of responsibilities for sensitive facilities.

### 4.3 Media Controls

Storage media that contain sensitive information must be controlled so that the information on the media is protected. This section addresses the protection, marking, sanitization, production input/output, and disposal of media containing sensitive information. Storage media include but are not limited to the following:

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

#### 4.3.1 Media Protection

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

All media containing sensitive information must be labeled and kept in a secure location.

Backup and archive media must be sent to an off-site location as identified in the appropriate business continuity and IT contingency plans.

DHS Policy
<b>a.</b> Components shall ensure all that media containing sensitive information, including hard copy media, backup media, and removable media such as USB drives, are stored in a secure location (e.g., a locked office, room, desk, bookcase, file cabinet, or other storage prohibiting access by unauthorized persons) when not in use.
<b>b.</b> Components shall ensure backup media are stored off site in accordance with their business continuity and IT Contingency plans.
<b>c.</b> DHS personnel and contractors are prohibited from using any non government issued removable media (USB drives, in particular) or connecting them to DHS equipment or networks or to store DHS sensitive information.

<b>DHS Policy</b>
-------------------

- |  |
|--|
| <p><b>d.</b> All DHS USB drives must be compliant with FIPS 140-2 and FIPS 197</p> |
|--|

Media protection responsibilities are provided below.

<b>Media Protection Responsibilities</b>
--

**CISO**

- Establishes and enforces DHS policy relating to labeling, storage, media reuse, and disposal of DHS equipment.

**System Owners**

- Ensure any special storage requirements are communicated to the IT project manager and system administrators.

**System/Network Administrators**

- Ensure that sensitive information is stored in a locked container or in an area with adequate access controls to prevent unauthorized access, disclosure, damage, modification, or destruction.
- Ensure that recipients of sensitive information have a valid “need to know” and proper authorization.
- Ensure that copies of backups are stored at secure offsite locations.

**Facility Managers**

- Ensure that sensitive information is stored in a locked container or in an area with adequate access controls to prevent unauthorized access, disclosure, damage, modification, or destruction.
- Establish both onsite and offsite storage locations.
- Establish and maintain an inventory accounting system for all media entering or leaving a media storage area. Inventory should be verified at least semiannually.
- Ensure that backup storage facilities meet the minimum requirements enumerated in Section 4.11, Information and Data Backup.

**ISSOs**

- Ensure that media are stored in accordance with the requirements enumerated in this handbook.
- Ensure that storage requirements are addressed in the Security Plan and rules of behavior.

### 4.3.2 Media Marking

DHS processes, stores, and transmits sensitive information, including investigative information, information that could be sold for profit, information that could result in physical risk to individuals, law enforcement information, and criminal information. Appropriately labeling the media containing such information ensures that all recipients of the material are aware that the information requires protection.

Note: It is important to remember that if information with different levels of sensitivity is combined, the total package must carry the sensitivity level of the information that has the greatest sensitivity.

The following definitions apply within this section:

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

It is recommended that a label be affixed to PCs, terminals, and laptop computers and other mobile computing devices not authorized to process classified information, especially in environments where both sensitive information and classified information are processed. Labels stating “this medium is unclassified” are available from GSA (standard form 710).

#### DHS Policy

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

Media marking responsibilities are provided below.

#### Media Marking Responsibilities

##### **CISO**

- Establishes and enforces policy relating to labeling, storage, reuse, and disposal of media containing DHS sensitive information.

##### **System Owners**

- Ensure that mission security needs based on the sensitivity of the information being processed are communicated to project managers and system administrators.

##### **IT Project Managers**

- Implement electronic marking requirements and warning banners for automated systems.

##### **System Administrators**

<b>Media Marking Responsibilities</b>
<ul style="list-style-type: none"> <li>• Implement electronic marking requirements and warning banners on their systems.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that sensitive systems and information are appropriately identified and that Sensitivity and Criticality levels are established for each system.</li> <li>• Ensure marking requirements are addressed in the System Security Plan and that noncompliance areas are identified.</li> <li>• Ensure that automated system and site personnel understand and are adequately trained in the identification of sensitive information and marking instructions.</li> <li>• Ensure that marking procedures and warning banners are reviewed with DHS employees on a periodic basis, such as during annual Computer Security Awareness sessions.</li> <li>• Ensure that all users are aware of the value and sensitivity of DHS information.</li> <li>• Ensure that users understand their responsibilities for safeguarding DHS information and how to fulfill their responsibilities.</li> <li>• Ensure that procedures are in place to ensure that DHS employees follow guidelines and procedures regarding marking.</li> </ul>

### 4.3.3 Media Sanitization and Disposal

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

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

Media sanitization responsibilities are provided below.

<b>Media Sanitization Responsibilities</b>
<p><b>Site Managers</b></p> <ul style="list-style-type: none"> <li>• Allocate resources to meet media sanitization requirements.</li> <li>• Enforce media sanitization requirements.</li> </ul> <p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Develop and implement media sanitization procedures for storage media to be disposed of or</li> </ul>

<b>Media Sanitization Responsibilities</b>
<p>recycled, reused, returned to the owner, or returned for repair or replacement.</p> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that media sanitization requirements are addressed in the System Security Plan and Security Operating Procedures.</li> <li>• Maintain records of the sanitization and disposition of sensitive storage media.</li> </ul> <p><b>System/Network Administrators</b></p> <ul style="list-style-type: none"> <li>• Ensure that storage media for disposal, recycling, or reuse are properly sanitized.</li> <li>• Ensure that leased storage media are properly sanitized before they are returned to the owner.</li> <li>• Ensure that defective or inoperable storage media are properly sanitized before they are returned to the vendor or manufacturer for repair or replacement. Ensure that defective or inoperable storage media that cannot be sanitized are physically destroyed and disposed of.</li> <li>• Periodically test degausser equipment to ensure proper operation.</li> </ul> <p><b>Users</b></p> <ul style="list-style-type: none"> <li>• Ensure the safekeeping of sensitive storage media in their possession.</li> <li>• Notify ISSO or Site Security Manager when media containing sensitive information are no longer required.</li> </ul>








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

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

The NIST guidelines apply to media containing sensitive information. The DHS 4300B National Security Systems Handbook provides information on the sanitization requirements for media containing classified information.

NIST SP 800-88 identifies sanitization options for various IT storage media. Sanitization options depend on the type of storage medium (e.g., hard drive, CD or DVD, hard copy), intended disposition of the medium (e.g., reuse, disposal), and FIPS 199 categorization for the confidentiality security objective (see Section 3.9.1, FIPS 199 Categorization and the NIST SP 800-53 Controls).

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

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

Overwriting cannot be used for magnetic media that are damaged or not writeable. In such cases, the media must be physically destroyed.

- **Purging:** the removal of information stored on media in such a way that the information is irretrievable through any means, including advanced laboratory techniques. For example, magnetic media such as hard drives and diskettes can be purged by degaussing. Degaussers expose the medium to a strong magnetic field, which effectively erases the information (however, a degausser designed and approved for the type of medium being purged is required). Note that degaussing destroys hard drives, as the firmware that manages the drive is also purged during the degaussing process.

Degaussing is effective only on magnetic media such as hard drives, diskettes, and magnetic tapes. It is not effective, for example, on optical media such as CDs and DVDs.

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

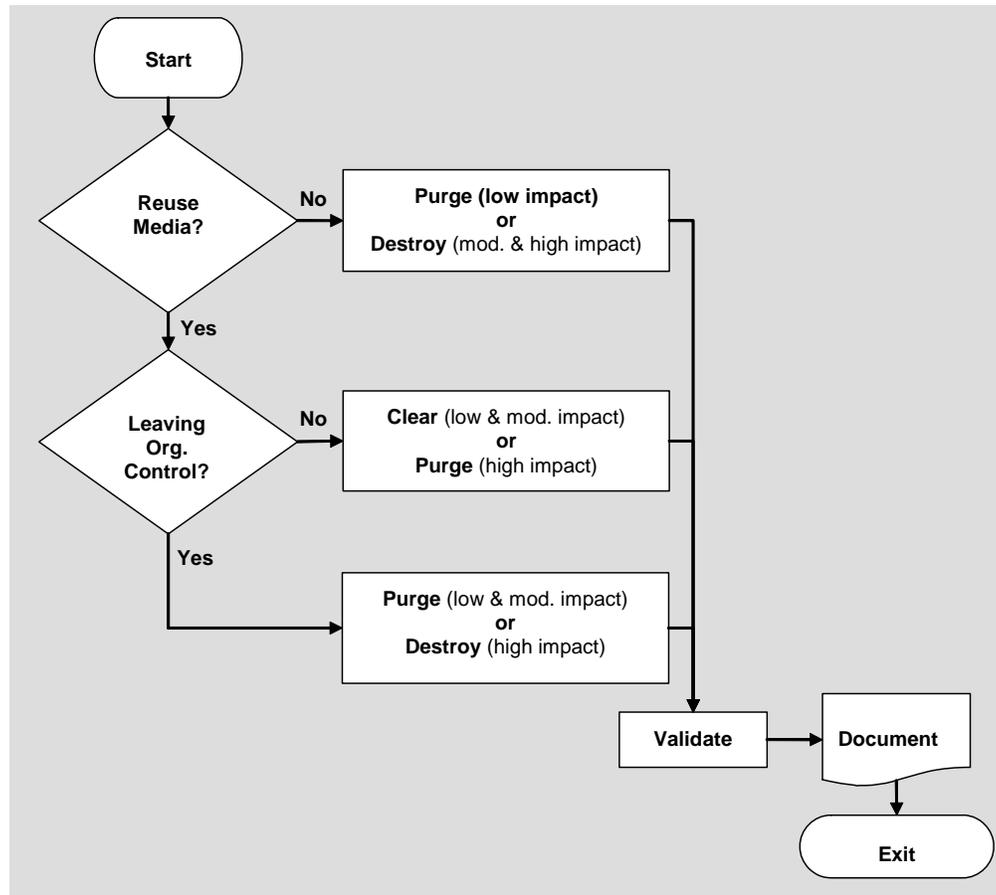
Sanitization also requires the removal of all labels, markings, and activity logs.

Steps for sanitizing of media are the following:

- Determine the categorization (i.e., low, moderate, or high impact) for the confidentiality security objective
- Determine whether the media will be disposed of or reused (either within or outside of the organization)
- Use Figure 3 to determine the appropriate method of sanitization

**Figure 3. Flowchart depicting the process for selecting media sanitization method, by categorization of impact for the confidentiality security objective.**

(Adapted from NIST SP 800-88.)



- Refer to Appendix A and Table A-1 in NIST SP 800-88 for sanitization options for the type of medium to be sanitized
- Validate and document the sanitization of the medium. Appendix F in NIST SP 800-88 provides a sample sanitization validation form

Sensitive media can be shipped to facilities for clearing, sanitization, or disposal following the guidelines in Section 4.3.4, Production, Input/Output Controls.

The National Security Agency (NSA) may accept sensitive media for destruction. For more information and for requirements, contact NSA Classified Material Conversion Customer Service at (301) 688-6672.

#### 4.3.4 Production, Input/Output Controls

Regardless of method, transmission of sensitive information should be effected through means that limit the potential for unauthorized public disclosure. Since information transmitted over unencrypted electronic links such as telephone lines may be intercepted by unintended recipients, custodians of sensitive information should decide whether specific information

warrants a higher level of protection afforded by a secure fax, secure phone, or other encrypted means of communication.

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

Responsibilities related to production, input/output controls are provided below.

<b>Production, Input/Output Control Responsibilities</b>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Develop and enforce policy relating to the input and output of DHS information.</li> </ul> <p><b>Facility Managers</b></p> <ul style="list-style-type: none"> <li>• Ensure that sensitive information is transmitted and received in accordance with DHS policy.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that the Security Plan addresses transmission of sensitive material.</li> <li>• Ensure that users have authority to access only information for which they have a valid “need to know.”</li> <li>• Ensure that sensitive information is transmitted in a secure manner.</li> </ul>

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

In data-center environments, procedures should be implemented to account for the receipt of input and output media to include paper and magnetic media. Authorization lists should be maintained identifying who is authorized to submit input for processing and receive output after processing. Logs should be maintained to document the transfer of sensitive data via a third party such as mail and courier services.

#### **4.4 Voice Communications Security**

This section addresses vulnerabilities inherent in voice communications and the operational controls needed to mitigate the risks associated with these vulnerabilities. Voice communication security encompasses Private Branch Exchange (PBX) systems, telephone usage, and voice mail. Note: In the event that Components choose to encrypt their voice communications, AES encryption per FIPS 140-2 must be used.

##### **4.4.1 Private Branch Exchange**

A PBX is a computer-based switch that acts as a small, in-house phone company for the organization that operates it. Failure to secure a PBX system can result in toll fraud as well as theft of proprietary, personal, and confidential information. Moreover, an attacker could also use

the call tracking features of an unsecured PBX for traffic analysis to determine possible patterns of response to a planned incursion. Protecting the PBX is thus a high priority.

### DHS Policy

Components shall provide adequate physical and IT security for all DHS-owned Private Branch Exchanges (PBX). (Refer to NIST SP 800-24, *PBX Vulnerability Analysis*, for guidance on detecting and fixing vulnerabilities in PBX systems.)

PBX security responsibilities are provided below.

### PBX Security Responsibilities

#### ISSMs

- Provide guidance concerning appropriate PBX-related security training to include:
  - Types of information personnel should not release to callers.
  - Security requirements for new PBX systems (e.g., disable test accounts, passwords, and shortcut keys) and for maintenance activities for distribution to vendors.

#### Site Managers

- Ensure that employees and others with access to the facilities have agreed to and signed a PBX policy statement.
- Ensure that the PBX contracts and maintenance agreements include information on disputes, how they are settled, and the appeals process. Obtain approval from legal team before implementing.
- Explicitly include the requirements for integrity, availability, and confidentiality protection in the PBX, and directly address liability in PBX contractual agreements.
- Develop specific guidelines on acceptable and unacceptable use of telecommunications within the organization, and specify how the PBX policy deals with actions not explicitly covered by the policy.

#### ISSOs

- Address PBX issues in annual awareness sessions provided to all employees.
- Identify the personnel or position(s) responsible for telephone usage in the PBX policy statement.
- Ensure that agreements with the local exchange carrier (LEC), the inter-exchange carrier (IXC), and the equipment vendors allow for only authorized personnel to request service level changes, and to report errors.
- Verify all toll calls billed against PBX traffic reports.
- Ensure that internal PBX audits include verifying that all records are in electronic form.
- Ensure that internal IT auditors complete an audit of each PBX system at least once a quarter.
- Ensure that all personnel with access to the PBX or connected equipment have signed employee agreements including PBX-related material.
- Test audit mechanisms at least quarterly.
- Test audit computers periodically.
- Ensure external auditors do blind external testing.

#### PBX Administrators

### **PBX Security Responsibilities**

- Identify the personnel or position(s) responsible for telephone usage in the PBX policy statement.
- Ensure that agreements with the LEC, the IXC, and the equipment vendors allow for only authorized personnel to request service level changes, and to report errors.
- Verify all toll calls billed against PBX traffic reports.
- Ensure that internal PBX audits include verifying that all records are in electronic form.
- Ensure that internal IT auditors complete an audit of each PBX system at least once a quarter.
- Ensure that all personnel with access to the PBX or connected equipment have signed employee agreements including PBX-related material.
- Test audit mechanisms at least quarterly.
- Test audit computers periodically.
- Ensure external auditors do blind external testing.

### **Site Telephone Technical Support**

- Clearly mark circuit numbers on channel banks, CSUs, DSUs, and modems.
- Clearly label main distribution frame (MDF)s and intermediate distribution frame (IDF)s.
- Fully document procedures for making PBX software and hardware changes and use signed checklists to record all changes as they occur.
- Identify third party calls on phone bills and flag them on automated analysis.
- Generate and keep full call audit records in paper and electronic forms.
- Follow procedures to ensure the periodic dump of all PBX parameters and automatic comparison to the previous dump; report differences to management.
- Follow procedures to determine the frequency of the periodic dump and comparison as a normal part of risk management.
- Store PBX backups off-site, verify the media by reading back in, and periodically test the media on backup equipment to assure that they work properly.
- Ensure a complete dump of internal parameters is reconciled with previous dumps after completion of remote maintenance.
- Record all transactions in an external computer system.
- Ensure systems cannot redirect incoming calls from outside lines to make outside calls.
- Record and print all call details.
- Store records on a write once read many (WORM) disk for additional assurance.

Potential threats to a PBX include:

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

- Traffic analysis.

PBXs are sophisticated computer systems that share many of the threats and vulnerabilities associated with general purpose operating systems. There are, however, two important ways in which PBX security differs from conventional operating system security:

1. **External access/control.** Like larger telephone switches, PBXs typically require remote maintenance by the vendor. Instead of relying on local administrators to make operating system updates and patches, organizations normally have updates installed remotely by the switch manufacturer. This requires remote maintenance ports and access to the switch by a potentially large pool of outside parties.
2. **Feature richness.** The wide variety of features available on PBXs, particularly administrative features and conference functions, allow for the possibility of unexpected attacks. A hacker may use a feature in a manner not intended by its designers to eavesdrop on sensitive conversations. Features may also interact in unpredictable ways, leading to system compromise even if each component of the system conforms to its security requirements and the system operation and administration are correct.

#### 4.4.1.1 Maintenance Vulnerabilities

PBX manufacturers may include features useful when on-site maintenance personnel cannot resolve problems. For example, the manufacturer could instruct the maintenance personnel to configure and connect a modem to the maintenance port. Use of such remote connections must be controlled (only made available as needed in response to a particular problem), logged, and supervised. The manufacturer may then be able to dial in and use certain special features to resolve the problems without sending a representative to the customer's location. Use of such remote connections must be controlled (only made available as needed in response to a particular problem), logged, and supervised. These types of features must not be accessible via accounts held privately by the manufacturer. Proper password procedures must be enforced, with the exception that passwords should expire in a shorter period (e.g., 30 days) or be single use (e.g., a secure remote access device). All such access and changes to the PBX data and configuration must be logged.

Examples of these special features include:

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

These features are subject to intrusion, and could provide dangerous access to the PBX, if known by the wrong persons. To mitigate the risks associated with these vulnerabilities, ISSOs and site managers must:

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

#### **4.4.1.2 Software Loading and Update Tampering**

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

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

#### **4.4.1.3 User Features**

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

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

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

- Connect the attendant console to the PBX with a different physical connection than that of the telephone instruments.

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

#### 4.4.2 Telephone Communications

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

<b>DHS Policy</b>
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 on unsecured telephones.

Telephone communications responsibilities are provided below.

<b>Telephone Communications Responsibilities</b>
<p><b>CISO</b></p> <ul style="list-style-type: none"> <li>• Establishes and enforces policy relating to telephone communications.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that users are aware of the telephone communications policy.</li> </ul> <p><b>Users</b></p> <ul style="list-style-type: none"> <li>• Adhere to the telephone communications policy not to discuss classified information over the telephone and to exercise care when discussing sensitive information.</li> </ul>

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

- Telephones that are “on-hook” can intercept voice communications by design, modification or attachment of monitoring devices.

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

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

#### 4.4.3 Voice Mail

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

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

For more information, refer to Section 4.4.1, Private Branch Exchange.

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

Voice mail responsibilities are provided below.

<b>Voice Mail Responsibilities</b>
<p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>Identify the personnel or position(s) responsible for telephone usage in the applicable voice communications policy statement.</li> </ul> <p><b>PBX Administrators</b></p> <ul style="list-style-type: none"> <li>Identify the personnel or position(s) responsible for telephone usage in the applicable voice communications policy statement.</li> <li>Ensure that telephone systems are configured to enable enforcement of minimum password requirements for voice mail.</li> </ul> <p><b>Telephone Users</b></p> <ul style="list-style-type: none"> <li>Create secure passwords that adhere to at least the minimum voice mail password requirements.</li> </ul>

## 4.5 Data Communications

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

### 4.5.1 Telecommunications Protection Techniques

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

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

Telecommunications protection responsibilities are provided below.

<b>Telecommunications Protection Responsibilities</b>
<p><b>CISO/ISSMs</b></p> <ul style="list-style-type: none"> <li>Advise DHS project managers in the selection of telecommunications protection techniques that would serve as an alternative to encryption for data transmission protection techniques.</li> </ul> <p><b>System Owners</b></p> <ul style="list-style-type: none"> <li>Select the telecommunications protection techniques that meet their security needs consistent with DHS security policies in the most cost-effective manner.</li> </ul>

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

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

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

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

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

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

#### **4.5.2 Facsimiles**

Facsimile technology was developed for scanning and transmitting documents or pages. Although facsimile is traditionally a telephony-based application, the technology has evolved to address the transmission of text or image files. Standards are under development for Internet-based fax using store-and-forward protocols and real-time connectivity between IP-connected fax gateways.

Facsimile inherently is not a secure means of communication, and faxes can easily be intercepted and decoded. Fax protocols provide neither authentication nor non-repudiation services, which allows fax traffic to be sent to or received by improper recipients. The commonly used Group III fax protocol implements support for proprietary and undocumented data exchange using a

feature called nonstandard facilities (NSF). Therefore, fax servers or fax modems attached to networks provide a potential means for network intrusion and penetration.

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

<b>DHS Policy</b>
<p><b>a.</b> 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.</p>
<p><b>b.</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.</p>

Facsimile responsibilities are provided below.

<b>Facsimile Responsibilities</b>
<p><b>CISO</b></p> <ul style="list-style-type: none"> <li>• Establishes and enforces policy relating to the use of DHS facsimile machines.</li> </ul>
<p><b>System/Network Administrators</b></p> <ul style="list-style-type: none"> <li>• Ensure that facsimile machines connected to DHS IT resources are protected and configured to prevent mishandling of sensitive information.</li> </ul>
<p><b>Facility Managers</b></p> <ul style="list-style-type: none"> <li>• Ensure that appropriate physical security requirements are implemented for facsimile machines.</li> </ul>
<p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that applicable IT security requirements are applied as necessary to facsimile machines.</li> <li>• Ensure that the Security Plan addresses facsimile machines connected to DHS IT systems.</li> </ul>

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

Anyone sending sensitive information should verify the recipient’s secure fax number immediately before sending. They should also ascertain that the intended recipient (or trusted subordinate) will be present to receive the fax as soon as it is sent. Sensitive information should never be sent to an unattended fax machine. Sensitive material should be sent from a machine that has the “memory” features turned off, so that the information cannot be accessed or retransmitted (possibly to an untrusted recipient) at a later time. All documents that are being transmitted should be appropriately labeled (see Sections 4.3.2 and 4.11 of this handbook). The reverse procedure should be used if the individual is receiving. All documents transmitted or received should be immediately removed from the fax machine room and appropriately stored.

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

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

### 4.5.3 Video Teleconferencing

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

<b>DHS Policy</b>
<b>a.</b> Components shall implement controls to ensure that only authorized individuals are able to participate in each videoconference.
<b>b.</b> Components shall ensure appropriate transmission protections, commensurate with the highest sensitivity of information to be discussed, are in place throughout any video teleconference.
<b>c.</b> Video teleconferencing equipment and software shall be disabled when not in use.

Video teleconferencing responsibilities are provided below.

<b>Video Teleconferencing Responsibilities</b>
<p><b>DAAs</b></p> <ul style="list-style-type: none"> <li>• Carefully weigh the risk associated with the use of video teleconferencing equipment connected to DHS IT systems prior to accreditation.</li> </ul>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Advise DHS personnel in the selection and secure use of video teleconferencing technologies.</li> </ul>
<p><b>Supervisors</b></p> <ul style="list-style-type: none"> <li>• Establish procedures to ensure only authorized attendees participate in teleconferencing sessions.</li> <li>• Ensure procedures are in place to disable video teleconferencing equipment when not in use.</li> <li>• Ensure procedures are in place to label and store videotapes recorded during the teleconferencing.</li> </ul>
<p><b>ISSOs/Teleconferencing Operators</b></p> <ul style="list-style-type: none"> <li>• Ensure video teleconferencing is addressed in the Security Plan if the equipment is connected to a DHS IT system.</li> <li>• Ensure video teleconferencing equipment is disabled and secure when not in use.</li> <li>• Ensure appropriate transmission protections are in place commensurate with the highest sensitivity of information to be discussed when conducting a video teleconferencing session.</li> </ul>
<p><b>Users</b></p>

<b>Video Teleconferencing Responsibilities</b>
<ul style="list-style-type: none"> <li>• Shall not discuss information during a teleconferencing session at a higher level of classification than that established for the conference.</li> </ul>



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

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

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

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

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

#### **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.

<b>DHS Policy</b>
<p><b>a.</b> Prior to implementing voice over data network technology, Components shall conduct rigorous risk</p>

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

Responsibilities related to voice over data networks are provided below.

<b>Voice Over Data Networks Responsibilities</b>
<p><b>IT Project Managers</b></p> <ul style="list-style-type: none"> <li>• Ensure the design of voice over data network implementations have sufficient redundancy to ensure network outages do not result in the loss of both voice and data communications.</li> <li>• Ensure appropriate identification and authentication controls, audit logging, and integrity controls are implemented on every component of their voice over data networks.</li> </ul>
<p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that the inherent risks of voice over data network technology are clearly identified in the Accreditation Package to include the business justification for their use.</li> <li>• Ensure physical access to voice over data network components is restricted to authorized personnel.</li> <li>• Ensure appropriate identification and authentication controls, audit logging, and integrity controls are implemented on every component of their voice over data networks.</li> <li>• Ensure audit logs are reviewed.</li> <li>• Ensure IT systems that employ VoIP technology have been certified and accredited for this purpose with residual risks clearly identified and addressed in the Accreditation Package.</li> </ul>
<p><b>Network/System Administrators</b></p> <ul style="list-style-type: none"> <li>• Ensure appropriate identification and authentication controls, audit logging, and integrity controls are properly configured on every component of their voice over data networks.</li> </ul>
<p><b>Facility Managers</b></p> <ul style="list-style-type: none"> <li>• Ensure physical access to voice over data network components is restricted to authorized personnel.</li> </ul>

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

The implementation of these technologies is thus discouraged. Prior to implementing voice over data network technology, Components must conduct rigorous risk assessments and security

testing and provide Department business justification for their use. Furthermore, any IT systems that employ this technology must be certified and accredited for this purpose with residual risks clearly identified in the Accreditation Package.

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

Information integrity is a significant security concern is information integrity. Frame Relay, Asynchronous Transfer Mode (ATM) and Digital Subscriber Line (DSL) facilities are usually provided by commercial entities. The fact that these links are not directly controlled by DHS staff mandates encryption of any data (including voice) that traverses these links. The contractual arrangements with these suppliers must specify that only United States citizens will be involved in the maintenance and operation of these links.

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

Voice over IP (VoIP) is a relatively new technology. As with most new technologies, there are numerous vendor-specific protocols and numerous standards in development. Many of the security issues related to VoIP are dependent upon vendor selection and architecture design. Rigorous testing and clear business justification should be completed before a DAA in any of the DHS Components approves the use of this technology.

#### **4.6 Wireless Communications**

Wireless communications technologies include the following:

- Wireless systems (e.g., wireless local area networks [WLAN], wireless wide area networks [WWAN], wireless personal area networks [WPAN], peer-to-peer wireless networks, IT systems that leverage commercial wireless services). Wireless systems include the transmission medium, stationary integrated devices, firmware, supporting services, and protocols.
- Wireless portable electronic devices (PED) capable of storing, processing, or transmitting sensitive information (e.g., personal digital assistants [PDA], smart telephones, two-way pagers, handheld radios, cellular telephones, personal communications services [PCS] devices, multifunctional wireless devices, portable audio/video recording devices with wireless capability, scanning devices, and 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, and technical investigative communications systems).
- Radio Frequency Identification (RFID).

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

The DHS Wireless Management Office (WMO) must be notified within 30 days of all wireless communications systems acquisitions. Components requesting waivers or exceptions to wireless communications policies shall follow the procedures outlined in Section 1.5, Waivers and Exceptions.

Components employing encryption on wireless technologies must implement and enforce a key management plan consistent with DHS PKI Policy Authority. The key management plan shall clearly define the practices, procedures, and techniques used to enforce the key management policy and functional requirements. Representative guidance may be drawn from the draft NIST SP 800-57, *Recommendation for Key Management – Part 2: Best Practices for Key Management Organization (2002)*.

For wireless technologies classified as general support systems or major applications, the key management plan must be addressed in the System Security Plan (SSP).

<b>DHS Policy</b>
<b>a.</b> Wireless communications technologies are generally prohibited from use within DHS unless the appropriate DAA specifically approves a technology and application.
<b>b.</b> Components using PKI-based encryption on wireless systems, wireless PEDs, and wireless tactical systems shall implement and maintain a key management plan approved by the DHS PKI Policy Authority.
<b>c.</b> The DHS WMO shall be notified within 30 days of all wireless communications systems acquisitions.

Wireless communications responsibilities are provided below.

<b>Wireless Communications Responsibilities</b>
<p><b>PKI Policy Authority</b></p> <ul style="list-style-type: none"> <li>• Establishes and enforces the security requirements detailed in the key management plan.</li> </ul> <p><b>DAAs</b></p> <ul style="list-style-type: none"> <li>• Specifically approve or prohibit the use of wireless communications technologies within the Department.</li> <li>• Approve the implementation and use of the key management plan at acceptable risk levels.</li> <li>• Ensure appropriate and effective security measures are included in the key management plan.</li> <li>• Approve migration plans for transitioning legacy wireless systems</li> <li>• Notify the WMO and the DHS Enterprise Architecture Center of Excellence (EACOE) of any approval action.</li> </ul> <p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Advise system owners and IT project managers concerning the implementation of key management</li> </ul>

<b>Wireless Communications Responsibilities</b>
<p>plans.</p> <ul style="list-style-type: none"> <li>• Enforce DHS key management policy and procedures.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure key management security controls and functional requirements are implemented.</li> <li>• Ensure security assessments are conducted to evaluate the effectiveness of security objectives and controls supported by the key management plan.</li> </ul> <p><b>System/Network Administrators</b></p> <ul style="list-style-type: none"> <li>• Implement and enforce technical security mechanisms specified in key management plan.</li> </ul> <p><b>DHS Managers, Supervisors, and Employees</b></p> <ul style="list-style-type: none"> <li>• Adhere to DHS policy concerning the use of wireless communications technologies within the Department.</li> <li>• Adhere to DHS policy concerning key management policy and procedures.</li> </ul> <p><b>CISO</b></p> <ul style="list-style-type: none"> <li>• Review waivers and exceptions to wireless systems policy.</li> <li>• Vet wireless security-related issues to the WMO.</li> </ul>












#### 4.6.1 Wireless Systems

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

Wireless systems allow mobile devices, wired devices, and other devices to process, store, or transmit sensitive information using radio frequency (RF) or infrared (IR) capabilities. Wireless systems are vulnerable to a number of traditional attacks and attacks specific to wireless technologies. These attacks fall into the following categories: unauthorized access, denial-of-service/jamming/interference, signal detection/eavesdropping, spoofing/masquerading, and message modification. The use of appropriate countermeasures will help ensure that wireless systems to be deployed will comply with DHS IT security policy.

DHS 4300A Attachment Q1, *Wireless Systems*, provides guidance for DHS Components to use in developing and implementing security for wireless systems.

<b>DHS Policy</b>
<p><b>a.</b> Annual security assessments shall be conducted on all approved wireless systems. Wireless security assessments shall enumerate vulnerabilities, risk statements, risk levels, and corrective actions.</p>
<p><b>b.</b> Risk mitigation plans shall be developed to address wireless security vulnerabilities. These plans shall prioritize corrective actions and implementation milestones in accordance with defined risk levels.</p>
<p><b>c.</b> Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless system being approved for use.</p>

<b>DHS Policy</b>
<p><b>d.</b> System Security Plans shall adopt a defense-in-depth strategy that integrates firewalls, screening routers, wireless intrusion detection systems, antivirus software, encryption, strong authentication, and cryptographic key management to ensure security solutions and secure connections to external interfaces are consistently enforced.</p>
<p><b>e.</b> Legacy wireless systems that are not compliant with DHS IT security policy shall implement a migration plan to outline the provisions, procedures, and restrictions for transitioning these systems to DHS-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception to policy from the CISO, as appropriate.</p>

Wireless system responsibilities are provided below.

<b>Wireless System Responsibilities</b>
<p><b>DAAs</b></p> <ul style="list-style-type: none"> <li>• Approve the use of standards-based wireless system technologies.</li> <li>• Approve the implementation and use of wireless systems at a specified risk level during the C&amp;A process.</li> <li>• Ensure appropriate and effective security measures are included in the System Security Plan.</li> </ul> <p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Advise System Owners and IT project managers concerning the implementation of wireless technologies.</li> <li>• Enforce DHS policy concerning wireless systems.</li> <li>• Enforce DHS policy concerning the reporting requirements for wireless security vulnerability assessments.</li> </ul> <p><b>System Owners/IT Project Managers</b></p> <ul style="list-style-type: none"> <li>• Develop risk mitigation plans for prioritizing corrective actions and implementation milestones.</li> <li>• Develop migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless systems to DHS-compliant security architectures.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure wireless systems security controls are properly implemented and configured and are addressed in the System Security Plan.</li> <li>• Ensure routine security assessments are accomplished on wireless systems to identify unauthorized wireless devices, backdoors, and other system vulnerabilities, and to enumerate vulnerabilities, risk statements, risk levels, and corrective actions.</li> <li>• Implement risk mitigation plans for prioritizing corrective actions and achieving implementation milestones.</li> <li>• Implement migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless systems to DHS-compliant security architectures.</li> </ul> <p><b>System/Network Administrators</b></p> <ul style="list-style-type: none"> <li>• Ensure wireless system security controls are properly implemented and configured in accordance with the System Security Plan.</li> </ul>

<b>Wireless System Responsibilities</b>
<ul style="list-style-type: none"> <li>• Ensure routine security assessments are accomplished on wireless systems to identify rogue access points, backdoors, and other system vulnerabilities, and to enumerate vulnerabilities, risk statements, risk levels, and corrective actions.</li> </ul> <p><b>DHS Managers, Supervisors, and Employees</b></p> <ul style="list-style-type: none"> <li>• Adhere to DHS policy concerning the use of wireless systems to process, store, or transmit sensitive information.</li> <li>• Adhere to DHS policy concerning the use of wireless systems in areas where sensitive information is being discussed.</li> </ul>






#### 4.6.2 Wireless Portable Electronic Devices

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

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

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

Government-owned PEDs can be used in conjunction with Department networks or systems (to include any downloading of data from a user's workstation to these devices) only if the current C&A documentation specifically addresses the inherent risks associated with their use and the DAA evaluates and accepts any residual risk. Re-certification and accreditation are required if these issues are not currently addressed in the most current C&A documentation.

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

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

Components are to develop and maintain a property inventory list of all PEDs authorized for use. This list is to include serial numbers and/or seat numbers, user names, use, and location of all PEDs for accountability purposes. Each DHS-owned PED is to have an asset tag, whose number

is included in the inventory list. Rules of behavior for PEDs must be published and enforced. DHS 4300A Attachment G provides guidance on developing rules of behavior, including rules for PEDs, and provides sample rules of behavior.

DHS 4300A Attachment Q2 (*Wireless Portable Electronic Devices*) provides guidance for DHS Components to use in developing and implementing wireless PED security.

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

<b>DHS Policy</b>
-------------------

in areas where sensitive information is discussed.
--

Wireless portable electronic device responsibilities are provided below.

<b>Wireless Portable Electronic Device Responsibilities</b>
---

**DAA**s

- Approve the use of Government-owned, DHS-approved wireless PEDs and accessory devices to connect, process, store, or transmit sensitive information.
- Ensure appropriate and effective security measures are included in the System Security Plan.
- Authorize the use of Government-owned wireless PEDS and accessory devices in areas where sensitive information is discussed.
- Evaluate the risk associated with authorizing wireless PEDs to connect, process, store, transmit, or access sensitive information and systems during the C&A process.
- Approve/disapprove the use of mobile code (e.g., ActiveX).

**System Owners/IT Project Managers**

- Develop risk mitigation plans for prioritizing corrective actions and implementation milestones.
- Develop migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless PEDs to DHS-compliant security architectures.
- Maintain an inventory of all approved wireless PEDs in operation.

**ISSMs**

- Enforce DHS policy on the use of wireless PEDs and accessory devices in areas where sensitive information is discussed.
- Enforce DHS policy concerning the use of wireless PEDs and accessory devices to connect, store, process, or transmit combinations, PINs, or sensitive information.
- Develop procedures for implementation of strong identification, authentication, data encryption, and transmission encryption for wireless PEDs to protect sensitive information from compromise.
- Enforce DHS policy concerning the use of mobile code and antivirus software on wireless PEDs.
- Identify and establish cost-effective countermeasures to denial-of-service attacks for wireless PEDs.

**ISSOs**

- Ensure wireless PEDs are not permitted in areas where sensitive information is discussed unless authorized in writing by the DAA.
- Enforce DHS policy concerning the use of wireless PEDs to process, store, or transmit sensitive information.
- Enforce DHS policy concerning the use of mobile code and antivirus software on wireless PEDs.
- Implement cost-effective countermeasures to denial-of-service attacks for wireless PEDs.
- Ensure that all information is cleared from wireless PEDs that are to be reused or surplus; ensure that all information is sanitized from wireless PEDs that are being disposed of, recycled, or returned to the owner or manufacturer (see Section 4.3.3, *Media Sanitization and Disposal*, for approved procedures).
- Implement migration plans that outline provisions, procedures, and restrictions for transitioning

<b>Wireless Portable Electronic Device Responsibilities</b>
<p>legacy wireless PEDs to DHS-compliant security architectures.</p> <ul style="list-style-type: none"> <li>• Enforce prohibition of add-on devices such as cameras and recorders.</li> </ul> <p><b>System/Network Administrators</b></p> <ul style="list-style-type: none"> <li>• Ensure wireless PED security controls are properly implemented and configured in accordance with the Systems Security Plan.</li> <li>• Ensure routine security assessments are accomplished on wireless PEDs.</li> </ul> <p><b>DHS Managers, Supervisors, and Employees</b></p> <ul style="list-style-type: none"> <li>• Adhere to DHS policy concerning the use of wireless PEDs in areas where sensitive information is being discussed.</li> <li>• Adhere to DHS policy concerning the use of wireless PEDs to process, store, transmit, or access combinations, PINs, or sensitive information.</li> </ul>

The differences among wireless PEDs are becoming less clear-cut as voice communications, email, calendars, text messaging, Internet capabilities, and other services converge on integrated PED platforms. These product innovations—while they improve mobility, flexibility, portability, and economies of scale—are subject to all the threats, vulnerabilities, and security risks inherent in evolving wireless technologies.

#### **4.6.2.1 Cellular Phones**

Cellular phones used in areas where sensitive information is discussed have the same inherent vulnerabilities as cordless telephones and speakerphones as discussed in Section 4.4.2. They potentially allow a discussion of sensitive information being held in the same area to be overheard by a third party who would not normally have access to such information.

As is the case with traditional telephones, cellular communications can be intercepted. However, the interception of conversations over telephones requires the insertion of a monitoring device; the interception of cellular communications does not, and information transmitted by cellular phones can be intercepted at reasonably great distances. An individual could be in a neighboring building or in the street outside the building and monitor conversations that are within the reach of the microphone in the cellular phone. In fact, cellular phone credentials can be cloned to other phones, allowing the “cloned” phone to masquerade as the original phone and allow covert monitoring of conversations near the original caller.

<b>DHS Policy</b>
<p>Components shall develop guidance for discussing sensitive information on cellular phones. Guidance shall be approved by a senior Component official and is subject to review by the DHS CISO and the DHS Wireless Management Office. Under no circumstances shall classified information be discussed on cellular phones.</p>

Cellular phone responsibilities are provided below.

<b>Cellular Phone Responsibilities</b>
<b>Managers</b>

<b>Cellular Phone Responsibilities</b>
<ul style="list-style-type: none"> <li>• Ensure employees are aware of DHS policy prohibiting the discussion of sensitive DHS information while using a wireless telephone.</li> </ul> <p><b>Users</b></p> <ul style="list-style-type: none"> <li>• Ensure sensitive DHS information is not discussed while using a wireless telephone.</li> </ul>

#### 4.6.2.2 Pagers

Text pagers can send text messages up to 110 or 160 characters long, depending on the carrier. Text messages also can be sent from a cellular service provider's Web page, or from Web sites that allow users to send text messages for free. Pagers have the same inherent vulnerabilities as cellular phones with respect to exposure of sensitive information to unauthorized recipients (see Section 4.6.2.1).

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

Pagers shall not be used to transmit information that is explicitly labeled as sensitive or classified. In addition, pagers should not be used to transmit information on computer or network problems or status. This information could be intercepted and used to identify the configuration and possibly the location of IT assets, which could be then be targeted for attack by an outsider or untrustworthy insider.

A preferred alternative to transmitting text messages is to page an individual with a phone number and require the individual to call that number using a traditional (i.e., noncellular or nonmobile) telephone in a location where the conversation could not be monitored by others in the immediate area and where sensitive information can safely be discussed.

<b>DHS Policy</b>
Pagers shall not be used to transmit sensitive information.

Pager responsibilities are provided below.

<b>Pager Responsibilities</b>
<p><b>Managers</b></p> <ul style="list-style-type: none"> <li>• Ensure employees are aware of DHS policy prohibiting the transmission of sensitive DHS information to pagers.</li> </ul> <p><b>Users</b></p> <ul style="list-style-type: none"> <li>• Ensure sensitive DHS information is not transmitted to pagers.</li> </ul>

### 4.6.2.3 Multifunctional Wireless Devices

Wireless devices have evolved to be multifunctional (cell phones, pagers, and radios can surf the Internet, retrieve email, take and transmit pictures, etc), and most of these functions have no security.

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

The risk assessment for multifunctional wireless devices is to include an assessment of the risks associated with all the functions, including infrared (IR), radio frequency (RF), and video. The DAA must approve the associated risks identified by the risk assessment. Based on the sensitivity and classification of the data and the associated risk from the risk assessment, the DAA may allow the use of multifunctional wireless devices.

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

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

Multifunctional wireless device responsibilities are provided below.

<b>Multifunctional Wireless Device Responsibilities</b>
<p><b>DAAs</b></p> <ul style="list-style-type: none"> <li>• Approve the implementation of multifunctional wireless devices at an acceptable level of risk.</li> <li>• Ensure that the System Security Plan adequately addresses the protection of sensitive material accessed and stored on multifunctional wireless devices prior to accreditation.</li> </ul> <p><b>IT Project Managers/System Owners</b></p> <ul style="list-style-type: none"> <li>• Ensure security requirements for multifunctional wireless devices are communicated to the IT project manager and system administrators.</li> </ul> <p><b>System/ Network Administrators</b></p> <ul style="list-style-type: none"> <li>• Ensure that multifunctional wireless devices are configured properly with encryption enabled to prevent unauthorized access, disclosure, damage, modification, or destruction of data.</li> <li>• Ensure multifunctional wireless devices are periodically scanned for rogue access points and other</li> </ul>

<b>Multifunctional Wireless Device Responsibilities</b>
<p>vulnerabilities.</p> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that the System Security Plan addresses the protection of sensitive material accessed and stored on wireless devices.</li> <li>• Ensure that security requirements for multifunctional wireless devices are addressed in the System Security Plan and rules of behavior.</li> <li>• Ensure routine security assessments are accomplished on multifunctional wireless devices to identify rogue access points, backdoors, and other system vulnerabilities, and to enumerate vulnerabilities, risk statements, risk levels, and corrective actions.</li> </ul>



### 4.6.3 Wireless Tactical Systems

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

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

LMR systems are the primary means of wireless communications for several DHS Components. Security and risk management principles must be included in every phase of the LMR system development lifecycle. LMR network communications traffic should include encryption and security controls such as those specified by NIST Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules* (May 2001), and FIPS 197, *Advanced Encryption Standard (AES)* (November 2001). LMR subscriber units can periodically update and rekey encryption protocols manually by using a handheld key variable loader (KVL) or automatically via OTAR techniques. With OTAR technology, radios can be rekeyed within seconds over the air from a remote location—allowing for easier and more regular rekeying, and resulting in improved security. In addition, the OTAR channel can be used for digital voice transmissions in the encrypted mode for emergency interoperability.

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

DHS 4300A Attachment Q3 (*Wireless Tactical Systems*) provides guidance for DHS Components to use in developing and implementing wireless tactical system security.

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

Wireless tactical system responsibilities are provided below.

<b>Wireless Tactical System Responsibilities</b>
<p><b>DAAs</b></p> <ul style="list-style-type: none"> <li>• Approve the use of wireless tactical systems technologies.</li> <li>• Approve the implementation and use of wireless tactical systems to process, store, or transmit sensitive information at acceptable risk levels during the C&amp;A process.</li> <li>• Ensure security measures are included in the System Security Plan.</li> <li>• Evaluate and submit waivers and exceptions to the CISO for wireless tactical systems when compliance with DHS IT security policy could potentially compromise tactical investigations, endanger personnel safety, or put the public at risk.</li> </ul> <p><b>System Owners/IT Project Managers</b></p> <ul style="list-style-type: none"> <li>• Implement cost-effective security measures specified in the System Security Plan including strong identification, authentication, and encryption.</li> <li>• Ensure the DAA is immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents.</li> <li>• Ensure allocation of resources to support security requirements and enforcement controls specified in the System Security Plan.</li> <li>• Ensure tactical wireless communication security requirements are communicated to ISSOs and</li> </ul>

### **Wireless Tactical System Responsibilities**

system administrators.

- Develop and implement migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless tactical systems to DHS-compliant security architectures.
- Maintain an inventory of all wireless tactical systems used to process, store, and transmit sensitive information.
- Ensure all LMR systems comply with Project 25 (P25, EIA/TIA-102) security standards where applicable.

#### **ISSMs**

- Enforce DHS policy concerning the use of tactical communication systems to process, store, transmit, or access sensitive information.
- Develop and enforce DHS policy concerning mitigation measures for denial-of-service (DoS) attacks.
- Enforce LMR system compliance with Project 25 (P25, EIA/TIA-102) security standards.

#### **ISSOs**

- Ensure the DAA is immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents.
- Implement DHS policy concerning the use of tactical communication devices to process, store, transmit, or access sensitive information.
- Ensure that any tactical communication devices used to process sensitive information are not permitted in conference rooms or secure facilities where sensitive information is discussed without written authorization from the DAA.
- Perform security assessments and validate the security posture of land mobile radio (LMR) subscriber units via over-the-air rekeying (OTAR) or hard rekeying using a crypto-period no longer than 180 days.
- Ensure that all information is cleared from wireless tactical systems that are to be reused or surplus; ensure that all information is sanitized from wireless tactical systems that are being disposed of, recycled, or returned to the owner or manufacturer (see Section 4.3.3, Media Sanitization and Disposal, for approved procedures).

#### **DHS Managers / Supervisors**

- Ensure the DAA is immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents.
- Ensure employees are aware of DHS policy and procedure for discussing sensitive information while using tactical communication devices.

#### **Employees**

- Adhere to DHS policy and procedures concerning the use of tactical communication devices that access, process, store, or transmit sensitive information and systems.

#### **4.6.4 Radio Frequency Identification (RFID)**

Radio Frequency Identification objects to be identified wirelessly over significant distances. Because of the computing limitations of RFID tags, it often is not feasible to implement many of the security mechanisms, such as cryptography and strong authentication that are commonly

supported on personal workstations, servers, and network infrastructure devices. RFID security controls can support Departmental and Component privacy objectives, mitigate risks to business processes, and prevent the disclosure of sensitive data.

DHS 4300A Attachment Q4 (*Sensitive RFID Systems*) provides guidance for DHS Components to use in developing and implementing RFID security.

<b>DHS Policy</b>
<b>a.</b> Components implementing RFID systems shall assess hazards of electromagnetic radiation to fuel, ordinance, and personnel before deployment of the RFID technology.
<b>b.</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.
<b>c.</b> 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.
<b>d.</b> 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.
<b>e.</b> When the RFID system is connected to a DHS data network, Components shall implement network security controls to appropriately segregate RFID network components such as RFID readers, middleware, and databases from other non-RFID network hosts.
<b>f.</b> Components implementing RFID technology shall determine whether or not tag cloning is a significant business risk. If such a significant risk exists, then tag transactions shall be cryptographically authenticated.

#### **4.7 Overseas Communications**

Overseas communications have different security requirements than domestic communications. The Department of State has published a series of Foreign Affairs Manuals relevant to this requirement.

<b>DHS Policy</b>
Where required or appropriate, all overseas communications shall be in accordance with the Department of State Foreign Affairs Manual (FAM), 12 FAM 600, <i>Information Security Technology</i> .

Overseas communications responsibilities are provided below.

<b>Overseas Communications Responsibilities</b>
<b>CISO</b>
<ul style="list-style-type: none"> <li>Establishes and enforces policy relating to overseas communications.</li> </ul>

<b>Overseas Communications Responsibilities</b>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Ensure Component IT systems under their purview comply with Department of State 12 FAM 600, <i>Information Security Technology</i>, for systems that communicate with overseas locations.</li> </ul> <p><b>IT Project Managers/System Owners</b></p> <ul style="list-style-type: none"> <li>• Ensure IT systems under their control or under development that will communicate with overseas locations comply with the requirements of Department of State 12 FAM 600, <i>Information Security Technology</i>.</li> </ul> <p><b>System/Network Administrators</b></p> <ul style="list-style-type: none"> <li>• Ensure that IT systems under their control that will communicate with overseas locations are properly configured and maintained to comply with the requirements of Department of State 12 FAM 600, <i>Information Security Technology</i>.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure IT systems under their control that communicate with overseas locations comply with Department of State 12 FAM 600, <i>Information Security Technology</i>.</li> </ul>










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

The following 600 Series Foreign Affairs Manuals are provided for reference along with their current Internet links:

- 12 FAM 610 Organization and Purpose of Computer Security (COMPUSEC)  
<http://www.foia.state.gov/masterdocs/12fam/12m0610.pdf>
- 12 FAM 620 Unclassified Automated Information Systems  
<http://www.foia.state.gov/masterdocs/12fam/12m0620.pdf>
- 12 FAM 630 Classified Automated Information Systems  
<http://www.foia.state.gov/masterdocs/12fam/12m0630.pdf>
- 12 FAM 640 Domestic and Overseas Automated Information Systems Connectivity  
<http://www.foia.state.gov/masterdocs/12fam/12m0640.pdf>
- 12 FAM 650 Acquisition Security Requirements for Operating Systems and Subsystem Components  
<http://www.foia.state.gov/masterdocs/12fam/12m0650.pdf>
- 12 FAM 660 Communications Security (this subchapter has been designated Sensitive—NOFORN and is not available via the Internet; contact the Department of State for a paper version)

## **4.8 Equipment**

This section addresses the use and maintenance of computer equipment. It stresses the importance of individual accountability in protecting these resources. Equipment security

encompasses workstations, laptops, other mobile computing devices, personally owned equipment, and the maintenance of these items.

#### 4.8.1 Workstations

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

<b>DHS Policy</b>
<b>a.</b> Components shall ensure that all unattended workstations are either logged off, locked, or use a password-protected screensaver, activated after 5 minutes of inactivity.
<b>b.</b> Components shall ensure that workstations are protected from theft.

Workstation responsibilities are provided below.

<b>Workstation Responsibilities</b>
<p><b>Facility Managers</b></p> <ul style="list-style-type: none"> <li>• Ensure physical security measures are adequate to protect computers (PCs, laptops, and servers) from theft.</li> </ul>
<p><b>Site Security Staff/ISSOs/Supervisors</b></p> <ul style="list-style-type: none"> <li>• Enforce DHS policy to secure workstations when unattended by users.</li> </ul>
<p><b>System/Network Administrators</b></p> <ul style="list-style-type: none"> <li>• Ensure workstations are configured for automatic logoff, or with automatic screensaver activation after 5 minutes of inactivity where possible.</li> </ul>
<p><b>Users</b></p> <ul style="list-style-type: none"> <li>• Adhere to DHS policy by securing workstations when unattended.</li> </ul>

System administrators and ISSOs must ensure that all users are educated in the proper procedures for logging off and for configuring screen savers. Specific procedures for logging off, locking workstations, and enabling password-protected screensavers are found in DHS 4300A Attachment I.

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

- Workstations must be adequately protected from theft.
- Only licensed and approved operating systems and applications can be used on DHS workstations.
- All default vendor or factory set administrator accounts and passwords shall be changed before installation or use.
- All equipment shall be marked with the highest level of classification of information that has ever been processed or stored on the device.

- Equipment must be housed in facilities authorized to process sensitive information.

#### 4.8.2 Laptop Computers and Other Mobile Computing Devices

DHS relies heavily on laptop computers and other mobile computing devices for conducting its business. The mobility of these devices has increased the productivity of the workforce, but at the same time has increased the risk of theft, unauthorized data disclosure, and virus infection. It is thus important to employ additional safeguard measures to protect these resources. This includes the laptops and other mobile computing devices themselves as well as the data processed and stored on these devices.

<b>DHS Policy</b>
<p><b>a.</b> Information stored on any laptop computer or other mobile computing device that may be used in a residence or on travel shall be encrypted using FIPS 140-2-approved encryption. Passwords and smart cards shall not be stored on or with the laptop or other mobile computing device.</p>
<p><b>b.</b> Laptop computers and other mobile computing devices in offices shall be secured when unattended via a locking cable, locked office, or locked cabinet or desk.</p>
<p><b>c.</b> Employees shall obtain the written approval of the office director before taking a laptop computer or other mobile computing device overseas.</p>

Responsibilities related to laptop computers and other mobile computing devices are provided below.

<b>Laptop Computer and Other Mobile Computing Device Responsibilities</b>
<p><b>CISO</b></p> <ul style="list-style-type: none"> <li>• Establishes DHS policy regarding the use of laptop computers and other mobile computing devices.</li> </ul>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Enforce DHS policy regarding the use of laptop computers and other mobile computing devices.</li> <li>• Provide technical expertise and evaluate the effectiveness of encryption methods for laptop computers and other mobile computing devices.</li> </ul>
<p><b>System/Network Administrators</b></p> <ul style="list-style-type: none"> <li>• Provide technical expertise and evaluate the effectiveness of encryption methods for laptop computers and other mobile computing devices.</li> <li>• Ensure that encryption technology is installed and properly configured on laptop computers and other mobile computing devices.</li> <li>• Assist ISSOs in implementing technical requirements for laptop computers and other mobile computing devices.</li> </ul>
<p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that security of laptop computers and other mobile computing devices is adequately addressed in the Security Plan.</li> <li>• Ensure users are aware of their responsibilities to adhere to the rules of behavior for laptop computers and other mobile computing devices.</li> </ul>

### **Laptop Computer and Other Mobile Computing Device Responsibilities**

- Ensure users are trained in the use of encryption for laptop computers and other mobile computing devices.
- Ensure physical security controls are in place for laptop computers and other mobile computing devices.
- Ensure the unique requirements of connection of laptop computers and other mobile computing devices to the network are addressed in the System Security Plan.
- Ensure that encryption methods employed on laptop computers and other mobile computing devices provide the protection required in the Security Plan.

#### **Users**

- Obtain written approval of the office director before taking a laptop computer or other mobile computing device overseas.
- Comply with the rules of behavior for laptop computers and other mobile computing devices.
- Utilize encryption technology provided for laptop computers and other mobile computing devices.
- Physically secure laptop computers and other mobile computing devices when not in use.
- Read and adhere to the laptop computer and other mobile computing device policies and procedures in this section and DHS 4300A Attachment G.
- Make supervisors and managers aware of any problems encountered in implementing laptop computer and other mobile computing device guidance and procedures.

The increased risk of theft of laptop computers and other mobile computing devices is both a security and a cost issue. There are significant costs associated with replacing the physical hardware as well as the costs of restoring the information residing on the device itself. The risk of data disclosure is also a major security concern. Thus, care must be taken to guard against theft at all times. Moreover, fundamental security principles must be followed when using laptop computers and other mobile computing devices. For example, a user's password should never be written down and stored with the device.

Laptop computers and other mobile computing devices cannot be connected to DHS networks or systems unless the network or system is certified and accredited for that functionality. The Security Plan must identify the devices that can be used to access the network or system, the purposes for the access, and the security controls to be employed for the connection. In addition, any laptop computers or other mobile computing devices that process sensitive data (whether or not they are connected to a DHS network) must employ virus protection. All diskettes must be scanned prior to use to ensure they are virus-free.

Rules of behavior for laptop computers and other mobile computing devices must be published and enforced. DHS 4300A Attachment G provides guidance on developing rules of behavior, including rules for laptop computers and other mobile computing devices, and provides sample rules of behavior.

Finally, laptop computers and other mobile computing devices that process sensitive data must employ encryption technology. Encryption policies and procedures are addressed in Section 5.5.1, Encryption.

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

Users shall not use personally owned equipment (e.g., laptop computers, PDAs) or software to process, access, or store sensitive information. Such equipment also includes plug-in and wireless (e.g., BlackBerry) peripherals that may employ removable media (e.g., CDs, DVDs). Also included are USB flash (thumb) drives, external drives, and diskettes. Additional policy and guidance pertaining to the protection and disposal of personally owned equipment and software is addressed in Section 4.3, Media Controls. Components shall ensure that this policy is reflected in appropriate rules of behavior documents and reinforced during periodic security awareness sessions.

<b>DHS Policy</b>
<p><b>a.</b> Personally owned equipment and software shall not be used to process, access, or store sensitive information without the written prior approval of the Designated Accrediting Authority (DAA).</p>
<p><b>b.</b> Equipment that is not owned or leased by the Federal Government, or operated by a contractor on behalf of the Federal Government, shall not be connected to DHS equipment or networks without the written prior approval of the Component ISSM.</p>

Responsibilities related to personally owned equipment and software are provided below.

<b>Personally Owned Equipment and Software Responsibilities</b>
<p><b>DAA's</b></p> <ul style="list-style-type: none"> <li>• Carefully evaluate the risk associated with authorizing the use of personally owned equipment or software.</li> </ul>
<p><b>ISSM's</b></p> <ul style="list-style-type: none"> <li>• Enforce DHS policy prohibiting the use of personally owned equipment to connect, process, store, or access sensitive information and systems.</li> </ul>
<p><b>ISSO's</b></p> <ul style="list-style-type: none"> <li>• Enforce DHS policy prohibiting the use of personally owned equipment to connect, process, store, or access sensitive information and systems.</li> <li>• Conduct reviews, at least semiannually, of all equipment and software in their respective offices to ensure that only Government-licensed software and equipment are being used.</li> <li>• Ensure that rules of behavior address policy regarding the use of personally owned equipment and software.</li> <li>• Ensure that security awareness sessions address policy regarding the use of personally owned equipment and software.</li> </ul>
<p><b>Users</b></p> <ul style="list-style-type: none"> <li>• Adhere to DHS policies prohibiting the use of personally owned equipment and software.</li> </ul>

No personally owned equipment is to be connected to DHS equipment. Exceptions require written approval from the DAA. Exceptions shall be made only when the DAA deems that the use or connection of personally owned equipment is essential to the Department's mission. The

DAA shall accept any risk associated with personally owned equipment and this residual risk must be documented as part of the C&A process.

Components shall conduct reviews, at least semiannually, of all equipment and software in their respective offices to ensure that only Government-licensed software and equipment are being used, or that appropriate exceptions have been documented.

#### 4.8.4 Hardware and Software

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

DHS has published secure baseline configuration guides for several operating systems, the Oracle 9i database management system, and CISCO routers (see Enclosure 1), and will provide additional configuration guides as required. These hardening guides provide system and database administrators with a clear, concise set of procedures that will ensure a minimum baseline of security in the installation and configuration of the hardware and software. These baselines represent the minimum configuration requirements; Components are authorized to implement more onerous configuration guides. These baselines were developed using a variety of security guidelines from the National Security Agency (NSA), the Defense Information Systems Agency (DISA), NIST (NIST SP 800-70: “Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers”), and other Federal agencies and from vendor recommendations.

Waivers to the requirements contained in the hardening guides should be requested using the Waivers and Exceptions Request Form (DHS 4300A Attachment B).

<b>DHS Policy</b>
<b>a.</b> Components shall ensure that the installation of hardware and software products meets the requirements specified in applicable DHS secure baseline configuration guides.
<b>b.</b> Components shall limit access to system software and hardware to authorized personnel.
<b>c.</b> Components shall test, authorize, and approve all new and revised software and hardware prior to implementation in accordance with their Configuration Management Plan.
<b>d.</b> Components shall manage systems to reduce vulnerabilities through vulnerability testing, promptly installing patches, and eliminating or disabling unnecessary services, if possible.
<b>e.</b> Maintenance ports shall be disabled and shall only be enabled during maintenance.

Hardware and software responsibilities are provided below.

<b>Hardware and Software Responsibilities</b>
<b>CISO/ISSMs</b>
<ul style="list-style-type: none"> <li>• Provide guidance in the preparation of secure baseline configuration guides for hardware and software; CISO approves secure baseline configuration guides.</li> </ul>
<b>DAA</b>

### **Hardware and Software Responsibilities**

- Ensures new hardware and software products have been approved and documented in the C&A documentation.

#### **ISSOs**

- Ensure adequate security measures are in place to protect access to hardware and software.
- Ensure new hardware and software products have been approved in accordance with the configuration management plan prior to installation.

#### **Network/ System Administrators**

- Ensure hardware and software are properly secured.
- Ensure maintenance ports are disabled when not in use.
- Ensure unnecessary services are disabled when possible.
- Scan system periodically to identify vulnerabilities and take corrective actions to reduce vulnerabilities.
- Test software security patches on a nonlive system prior to implementation on active production systems.
- Ensure new hardware and software products have been approved in accordance with the configuration management plan prior to installation.

#### **Facility Managers**

- Ensure adequate physical security measures are in place to protect access to hardware and software.
- Ensure access control policy is enforced.

#### **System Owners/IT Project Managers**

- Ensure that the installation of hardware and software products meets the configuration requirements specified in applicable DHS secure baseline configuration guides.

System maintenance requires either physical or logical access to the system. One of the most common methods hackers use to break into systems is through maintenance accounts that still have factory-set or easily guessed passwords. War-dialing techniques will also reveal maintenance ports that are not protected.

Only authorized personnel are to be granted access to system software and hardware in DHS. All authorized personnel must have appropriate security clearances prior to receiving access to system software and hardware. This requirement includes maintenance personnel.

Affected systems are to be backed up before maintenance begins, and changes made to hardware or software during maintenance are to be logged. All new or revised software and hardware must be tested, authorized, and approved in accordance with the configuration management plan. New hardware and software must be documented in the C&A package and approved by the DAA. Following IT system upgrades or consolidations, surplus equipment must be secured until it has been prepared for surplus.

As outlined in Section 5.4.8, vulnerability testing must be conducted regularly to identify existing vulnerabilities. Patches are to be installed, after testing in a nonlive environment, as they become available. All unnecessary services provided by the operating system must be

disabled, if possible. Finally, maintenance ports must be disabled and enabled only during maintenance.

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

This section discusses DHS policies applicable to the personal use of Government office equipment and DHS IT systems/computers. Policies governing personal use are derived from several DHS management directives.

<b>DHS Policy</b>
<p><b>a.</b> DHS employees may use Government office equipment and DHS IT systems/computers for authorized purposes only. “Authorized use” includes limited personal use as described in DHS MD 4600.1, <i>Personal Use of Government Office Equipment</i>, and DHS MD 4900, <i>Individual Use and Operation of DHS Information Systems/Computers</i>.</p>
<p><b>b.</b> Limited personal use of DHS email and Internet services is authorized for DHS employees as long as this use does not interfere with official duties or cause degradation of network services. DHS users must comply with the provisions of DHS MD 4500, <i>DHS E-Mail Usage</i>, and DHS MD 4400.1, <i>DHS Web and Information Systems</i>.</p>
<p><b>c.</b> DHS users do not have any right to or expectation of privacy while using Government office equipment and/or DHS IT systems/computers, including Internet and email services.</p>
<p><b>d.</b> The use of Government office equipment and DHS IT systems/computers constitutes consent to monitoring and auditing of the equipment/systems at all times. Monitoring includes the tracking of internal transactions and external transactions such as Internet access. It also includes auditing of stored data on local and network storage devices as well as removable media.</p>
<p><b>e.</b> DHS users are required to sign rules of behavior prior to being granted IT accounts or access to DHS IT systems or data. The rules of behavior shall contain a “Consent to Monitor” provision and an acknowledgement that the user has no expectation of privacy.</p>
<p><b>f.</b> Contractors or other non-DHS employees are not authorized to use Government office equipment or IT systems/computers for personal use, unless limited personal use is specifically permitted by the 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.</p>

Responsibilities related to personal use of Government office equipment and DHS IT systems/computers are provided below.

<b>Personal Use of Government Office Equipment and DHS IT Systems/Computers Responsibilities</b>
<p><b>Human Capital Office</b></p> <ul style="list-style-type: none"> <li>• Establishes DHS policy regarding personal use of Government resources.</li> </ul>
<p><b>CIO/CISO</b></p> <ul style="list-style-type: none"> <li>• Provide policy and guidance concerning appropriate use of computer resources.</li> </ul>

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

- Establish and implement appropriate enforcement policies for noncompliance with computer resource usage policies.

**ISSMs**

- Ensure that controls, including awareness training, are in place to minimize or prevent unauthorized use of Government resources.

**Supervisors**

- Enforce personal use policies, including remedial training and other sanctions.
- Promptly report unauthorized use of Government resources in accordance with DHS incident reporting procedures (see DHS 4300A Attachment F).

**ISSOs, Network/System Administrators**

- As needed, remind users of their system responsibilities and the potential penalties for misuse of system resources; remind users that they do not have any right to or expectation of privacy while using Government office equipment and/or DHS IT systems/computers, including Internet and email services.

**Users**

- Be aware of the personal use policies described in this section of the handbook and in other references provided by DHS security officials, including the *Standards of Ethical Conduct for Employees of the Executive Branch*.
- Adhere to personal use policies established in this section and in other references provided by DHS security officials.
- Promptly report unauthorized use of Government resources in accordance with DHS incident reporting procedures (see DHS 4300A Attachment F).
- Be aware of and understand the disciplinary actions associated with violations of IT security policy, including the unauthorized use of Government resources.
- Should NOT have any expectation of privacy in the use of Government computers or computer systems.

**Contractors and non-DHS Employee Users**

- Understand and abide by the personal use provisions of the contract or memorandum of agreement with DHS.

The use of Government-furnished property, including but not limited to office equipment, supplies, computer equipment, software, telecommunications devices, networks, and IT systems, is for official, authorized purposes only. Some limited personal use is allowed, but only when such use:

- Involves minimal additional expense to the Government
- Is performed on the employee's non-work time
- Does not reduce productivity or interfere with the mission or operations of DHS
- Does not violate the *Standards of Ethical Conduct for Employees of the Executive Branch*

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

- Use of Internet sites resulting in an additional charge to the Government
- Obtaining, viewing, or transmitting sexually explicit material or other material inappropriate to the workplace, which might be considered to contribute to a hostile work environment for some employees
- Use for other than official Governmental business that results in significant strain on Department computer systems (e.g., mass mailings or sending or downloading large files such as programs, pictures, video files, or games)
- Any otherwise prohibited activity, such as sending out solicitations or engaging in political activity prohibited by the Hatch Act

A more complete list of inappropriate uses is contained in MD 4600.1.

Inappropriate use is considered a security incident. Depending on its severity, the incident may be deemed a security violation and, as such, be reportable under the DHS SOC/CSIRC provisions of Section 4.9 and DHS 4300A Attachment F.

Failure to adhere to DHS personal use policies can also result in sanctions. 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. IT security-related violations are addressed in the *Standards of Ethical Conduct for Employees of the Executive Branch*.

Employees should NOT expect privacy when using Government resources. To the extent that employees wish their private activities to remain private, they should avoid using DHS computer systems for such activities. A banner message indicating this policy will be displayed on the login screens of DHS computers. This information will also be included in the Rules of Behavior that users are required to sign on an annual basis.

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

Contractors are not authorized to use Government office equipment or IT systems/computers for personal use under any circumstances, unless limited personal use is specifically permitted by the contract. When so authorized, contractors shall be governed by the limited personal use policies of this section.

#### **4.8.6 Wireless Settings for Peripheral Equipment**

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

<b>DHS Policy</b>
<p><b>a.</b> Components shall ensure that wireless capabilities for peripheral equipment are disabled. This applies all to peripherals connected to any DHS network or to systems processing or hosting DHS sensitive data.</p>
<p><b>b.</b> In cases where valid mission requirements or equipment limitations prevent disabling wireless capabilities, Components shall comply with all requirements outlined in Section 4.6, Wireless Communication <i>and</i> obtain a waiver or exception in accordance with Section 1.5, Exceptions and Waivers.</p>

#### **4.9 Security Incidents and Incident Response and Reporting**

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

Over the last decade both the Government and private industry have become increasingly reliant on computer and networking resources. At the same time, attacks against these automated systems have increased dramatically. As reliance on computer resources has increased, the systems that process the information critical to these organizations have become more vulnerable to attack, viruses, system failure, and user error. These problems have occurred within both high- and low-profile organizations and have occurred regardless of the sensitivity and criticality of the data being processed.

Incidents can be accidental or malicious, can be caused by outside intruders or internal employees, and can cause significant disruptions to mission critical business processes. These incidents can severely disrupt computer-supported operations, compromise the confidentiality of sensitive information, and diminish the integrity of critical data. The effects of security incidents can range from embarrassment, interruption of service, inability to function, and, potentially, to loss of human life. According to a General Accounting Office (GAO) October 2001 report, *Information Sharing: Practices that Can Benefit Critical Infrastructure Protection*, a significant concern is that terrorists or hostile foreign states could severely damage or disrupt critical operations, resulting in harm to the public welfare.

To help combat the disruptive short- and long-term effects of security incidents, direction from higher authority requires that each Government agency implement and maintain a security incident reporting and handling capability. Examples of this direction include the following:

- OMB Circular A-130 specifies that Federal agencies will “Ensure there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats.”
- Homeland Security Presidential Directive 7 (Hspd-7) directs that each Department and agency will identify and provide information security protections commensurate with the risk

and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

- The Federal Information Security Management Act of 2002 (FISMA) directs that a program for detecting, reporting, and responding to security incidents be established in each Department. FISMA also requires the establishment of a central Federal information security incident center. This center is the U.S. Computer Emergency Readiness Team (US-CERT), established in 2003 within DHS.

In addition, OMB M-06-19 (Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments) requires that agencies report *all* incidents involving personally identifiable information to US-CERT within one hour of discovery of the incident. All incidents involving personally identifiable information in electronic or physical form are to be reported, and no distinction is to be made between suspected and confirmed breaches. US-CERT will forward all agency reports to the appropriate Identity Theft Task Force point of contact also within one hour of notification by an agency.

<b>DHS Policy</b>
<b>a.</b> Components shall establish and maintain a Component incident response capability.
<b>b.</b> Components shall report <i>significant incidents</i> to the DHS SOC as soon as possible via phone (703-921-6505) but not later than one hour from “validation,” e.g. a security event being confirmed as a security incident. Other means of communication, such as the SOC portal ( <a href="https://soconline.dhs.gov">https://soconline.dhs.gov</a> ) (Accessible only via the DHS Intranet), are acceptable, but the Component is responsible for <u>positively verifying</u> that the notification is received and acknowledged by the DHS SOC.
<b>c.</b> Significant HSDN incidents shall be documented with a preliminary report that will be provided to the HSDN GWO or DHS CSIRC within one hour. An initial report detail will be provided to DHS CSIRC within four hours. Subsequent updates and status reports will be provided to DHS CSIRC every 24 hours until incident resolution or when new information is discovered. Significant incidents are reported individually on a per incident basis and will not be reported in the monthly summary report. Refer to DHS 4300A Attachment H Section 2.6 for guidance.
<b>d.</b> Components shall report minor incidents on systems in the weekly incident report. FOUO systems may report via the DHS SOC portal ( <a href="https://soconline.dhs.gov">https://soconline.dhs.gov</a> ) (Accessible only via the DHS Intranet). Components with no portal access will report minor incidents via email to <a href="mailto:dhs.soc@dhs.gov">dhs.soc@dhs.gov</a> . HSDN incidents will be documented in a summary report provided to the HSDN GWO or DHS CSIRC on a weekly basis
<b>e.</b> All reports must be classified at the highest classification level of the information contained in the document. Unsanitized reports are marked and handled appropriately. Refer to MD4300A Attachment F for guidance.
<b>f.</b> If a DHS Component has no incidents to report for a given week, a weekly “No Incidents” report shall be sent via the DHS SOC portal ( <a href="https://soconline.dhs.gov">https://soconline.dhs.gov</a> ) (Accessible only via the DHS Intranet). Components with no portal access will report minor incidents via email sent to <a href="mailto:dhs.soc@dhs.gov">dhs.soc@dhs.gov</a> .
<b>g.</b> The DHS CSIRC shall report incidents to US-CERT, in accordance with the US-CERT CONOPS,

DHS Policy
as they arrive. Components should not send incident reports directly to US-CERT.

Security incident response and reporting responsibilities are provided below.

Security Incident Response and Reporting Responsibilities
<p><b>CIO</b></p> <ul style="list-style-type: none"> <li>• Determines whether or not security incident information is releasable to the public.</li> </ul> <p><b>CISO</b></p> <ul style="list-style-type: none"> <li>• Manages the DHS SOC/CSIRC and the incident reporting program.</li> <li>• Advises the CIO on status of significant incident activity.</li> <li>• Advises the CIO on the outcome of incident investigations.</li> <li>• Distributes incident reports to each Component.</li> </ul> <p><b>SOC/CSIRC</b></p> <ul style="list-style-type: none"> <li>• Serves as the focal point for all DHS incident response activities, to include reporting, incident response, and remediation.</li> </ul> <p><b>ISSM</b></p> <ul style="list-style-type: none"> <li>• Ensures compliance with DHS incident reporting and violation handling policies.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that system development and site personnel submit incident reports as specified in this section of the handbook.</li> <li>• Ensure that system development personnel and system users are trained in the proper procedures for recognizing and reporting security incidents in accordance with the requirements in DHS 4300A Attachment F, <i>Incident Response and Reporting</i>.</li> </ul> <p><b>System/LAN Administrators</b></p> <ul style="list-style-type: none"> <li>• Promptly report computer security incidents in accordance with DHS incident reporting procedures (see DHS 4300A Attachment F).</li> </ul> <p><b>Users</b></p> <ul style="list-style-type: none"> <li>• Promptly report IT security incidents in accordance with DHS incident reporting procedures (see DHS 4300A Attachment F).</li> </ul>
















#### 4.9.1 Law Enforcement Incident Response

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

## 4.9.2 Definitions and Incident Categories

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

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

- Use of Internet sites that result in an additional charge to the Government
- Obtaining, viewing, or transmitting sexually explicit material or other material inappropriate to the workplace, which might be considered to contribute to a hostile work environment for some employees
- Use for other than official Governmental business that results in significant strain on Department computer systems (e.g., mass mailings or sending or downloading large files such as programs, pictures, video files, or games)
- Any otherwise prohibited activity, such as sending out solicitations or engaging in political activity prohibited by the Hatch Act

Sometimes, the security incident is a clear violation of an explicit or implied security policy in a computing or telecommunications system or network. DHS has identified several categories of computer security incident and defined them in DHS 4300A Attachment F. Examples include:

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

Categories of incidents include the following:

- **Unauthorized Access (Intrusion).** Unauthorized access includes all successful unauthorized accesses and suspicious unsuccessful attempts.
- **Denial of Service.** Denial of service attacks include incidents that affect the availability of critical resources such as email servers, Web servers, routers, gateways, or communications infrastructure.
- **Malicious Logic.** Malicious logic includes active code such as viruses, Trojan horses, worms, and scripts used by crackers/hackers to gain privileges and/or information, to capture passwords, and to modify audit logs to hide unauthorized activity.
- **Misuse.** A user violates Federal laws or regulations and/or Departmental policies regarding proper use of computer resources, installs unauthorized or unlicensed software, accesses resources and/or privileges that are greater than those assigned.

- PII Incident. Incidents involving personally identifiable information in electronic or physical form, including suspected and confirmed breaches.
- Probes and Reconnaissance Scans. Include probing or scanning networks for critical services or security weaknesses, also include nuisance scans.
- Classified System Incident. Any incident that involves a system used to process national security information.
- Alteration/Compromise of Information. Any incident that involves the unauthorized altering of information, or any incident that involves the compromise of information.
- Multiple Component. Any incident involving events considered significant incidents in more than one of the above categories.

#### **4.9.3 DHS Security Operations Center**

The DHS Security Operations Center (SOC) coordinates Department-level incident response and reporting, assists DHS Components with incident response, and identifies and resolves computer security irregularities that affect the ability of DHS to conduct its mission. The DHS SOC:

- Provides a 24-hour, seven-day-a-week point of contact for security incidents within the DHS
- Coordinates incident response with the external agencies, law enforcement, and US-CERT
- Administers, monitors, and reports on DHS backbone security tools (IDS, firewall, encryption, etc.) up to the point of entry into DHS networks
- Coordinates Department-wide security incident response
- Facilitates communications among experts working to resolve IT security issues
- Establishes and maintains a structured incident reporting and response process, and serves as the central point for identifying and correcting computer system vulnerabilities
- Coordinates with appropriate DHS and other agency law enforcement organizations should an incident require law enforcement involvement
- Provides IT security guidance, assistance, and feedback to DHS Components in the form of “lessons learned” reports, trend analyses, alerts and advisories, and technical recommendations
- Assists each Component and DHS Headquarters in the evaluation and the strengthening of in-place security measures
- Coordinates with research activities and other incident response entities in order to remain current with the latest threat and vulnerability technologies

Detailed procedures for identifying, reporting, and tracking incidents are provided in DHS 4300A Attachment F, *Incident Response and Reporting*.

#### **4.10 Documentation (Manuals, Network Diagrams)**

Documentation of IT systems involves the collection of detailed information, including functionality, system mission, unique personnel requirements, type of data processed,

architectural design, system interfaces, system boundaries, hardware and software components, system and network diagrams, cost of assets, system communications and facilities, and any additional system-specific information. This information represents the foundation of the configuration baseline of the system. All proposed changes to the configuration baseline must be analyzed and tested to determine if they have security implications. This includes all proposed configuration changes to operating systems, operating system security features, applications, critical system files, and system devices. Changes must be approved through a formal configuration change control board and documented before they are implemented.

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

Documentation responsibilities are provided below.

<b>Documentation Responsibilities</b>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Ensure that security issues are formally documented and tracked during the SDLC process.</li> </ul> <p><b>IT Project Managers/ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that change control procedures are documented and implemented for all proposed configuration changes to IT systems.</li> <li>• Ensure that all proposed configuration changes to operating systems, operating system security features, applications, critical system files, and system devices are formally approved and documented prior to the change being implemented.</li> <li>• Maintain a capability to quickly approve and implement time-sensitive security patches in reaction to late-breaking security vulnerabilities identified by the DHS CSIRC.</li> <li>• Ensure that all approved changes to the configuration baseline are documented, reviewed for accuracy, and that records are maintained for each IT system for both the current and all previous configurations.</li> <li>• Ensure that formal system configuration reviews are performed.</li> <li>• Ensure that accurate system documentation and configuration logs are maintained to reflect current and prior configuration baselines.</li> </ul>

Change control policies must take into account and have provisions for quickly testing and approving time-sensitive changes that result from newly released vulnerability information. Often in today's climate, severe new vulnerabilities quickly present themselves, and the risk of not immediately implementing the vendor-supplied patch exceeds the risk of installing an

untested vendor patch. DHS Components must have provisions for reacting quickly as these critical patches are identified and released by the DHS CSIRC.

Documentation of the IT system also encompasses its security features. The software, firmware, algorithms, data structures, processes, and other design mechanisms that satisfy a set of documented security requirements represent the security baseline of the system. Prior to the system being placed in the operational environment, default settings of the security components are to be set to the most restrictive mode for operational systems.

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

#### 4.11 Information and Data Backup

Adhering to requirements regarding data backups can significantly reduce the risk that data will be compromised or lost in the event of a disaster or other interruption of service. A Backup Operations Plan must be included in the Contingency Plan, as discussed in Section 3.5.3, Information Technology Contingency Planning.

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

Information and data backup responsibilities are provided below.

<b>Information and Data Backup Responsibilities</b>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Establish and enforce backup policy.</li> <li>• Provide technical expertise and evaluate the effectiveness of backup approaches.</li> </ul> <p><b>Certifying Officials</b></p> <ul style="list-style-type: none"> <li>• Ensure that a Backup Operations Plan is included in the Contingency Plan.</li> </ul> <p><b>System Owners</b></p> <ul style="list-style-type: none"> <li>• Ensure that a backup strategy and procedures are established, implemented, and tested in accordance with the contingency plan.</li> </ul> <p><b>System/Network Administrators</b></p> <ul style="list-style-type: none"> <li>• Ensure that regular (daily, weekly, monthly) backups are performed in accordance with system requirements.</li> <li>• Ensure that analyses are performed to determine the volume of data to be backed up, frequency of</li> </ul>

### Information and Data Backup Responsibilities

data modifications and updates, and access needs of the user community.

- Maintain a proper rotation strategy for backups.
- Ensure that all backup tapes are properly labeled in accordance with the highest data sensitivity level assigned to the system.
- Ensure that on-site and off-site backup storage locations are available.
- Ensure that on-site backups are stored in fire and water-proof containers.
- Ensure that at least one backup copy of system software is retained off-site.

#### ISSOs

- Ensure that a Backup Operations Plan is included in the Contingency Plan.
- Ensure that the Backup Operations Plan is tested *at least annually* and more frequently if the risk and magnitude of loss is sufficient to warrant doing so. Ensure that timely corrective actions are taken to address deficiencies discovered during testing.
- Ensure that on-site and off-site backup storage locations are available, that on-site backups are stored in fire and water-proof containers and that at least one back-up copy of system software is retained off-site.
- Ensure that users are apprised of their responsibilities with regard to backing up any sensitive data residing on their hard drives.
- Review the Contingency Plan as part of the accreditation process.
- Ensure users and system administrators understand their responsibilities and are aware of negative impacts that can result from failing to adequately back up critical data
- Ensure the Contingency Plan, including backup procedures, is tested at least annually and that timely corrective action is taken to address deficiencies discovered during testing.
- Ensure that all testing is formally documented and ensure that records are maintained as part of the system history.

#### Users

- Understand the critical nature of backing up sensitive data.
- Never keep critical data on individual hard drives unless a backup copy exists, preferably on the network.
- Keep supervisors apprised of projects in which critical data may not be adequately backed up.

Development of a data backup strategy begins early in the life cycle when the *criticality/sensitivity* of the system is first considered. The following factors (derived from the Risk Assessment and documented in the Contingency Plan) will drive the data backup strategy:

- Application restoration priorities based on DHS mission criticality
- The maximum amount of permissible downtime before DHS mission requirements are seriously degraded
- The amount of data updates that can be lost between a service interruption event and the last data backup

- The amount of changes in system configuration settings that can be lost between a service interruption event and the last data backup
- Interdependencies with other systems
- Who the system owners are

Elements that must be considered as part of the backup operations strategy include:

- Specific needs of the site
- People, their roles, responsibilities, and skill levels
- Hardware requirements
- Communications considerations
- Supplies required
- Location and availability of an alternate processing site
- Transportation requirements
- Space requirements of the recovery site
- Power and environmental requirements
- Backup documentation requirements.

the frequency of backups will depend upon how often the data processed by the system(s) changes and how important those changes are. Again, the risk assessment will drive this element of the backup strategy. Data backups need to be stored both on-site and off-site, in a secure facility, in fireproof and waterproof containers.

Data backup and restoration procedures must be tested at least quarterly as an integral part of testing the overall Contingency Plan. This will include testing backup copies to make sure they are actually usable for restoration. More frequent testing may be required commensurate with the risk and magnitude of loss or harm that could result from disruption of information processing support. Testing helps ensure that each person with data backup responsibilities understands and is able to technically fulfill his or her backup and recovery duties. Testing of data backup and restoration procedures needs to be formally documented and records of testing need to be retained as part of the system history.

The same principles that govern backup of system data also apply to individual users. Virtually all DHS employees and contractors will frequently possess critical sensitive data that resides on hard drives on Government-owned personal computers or laptops. Hard drive crashes combined with a failure to save critical files can result in a negative impact to the DHS mission or, at a minimum, result in additional costs and lost time to recover or duplicate lost data. Critical data should never be kept on individual hard drives unless a backup copy exists. The backup should preferably be stored on a network drive where frequent backups are made. DHS system administrators do not have the responsibility or the resources to assist users in recovering lost data resulting from hard drive crashes unless the system owner deems that said data is critical to a DHS mission.

## 4.12 Converging Technologies

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

<b>DHS Policy</b>
The policies in this document, including C&A requirements, apply to any devices that contain information technology, including copiers, fax machines, and HVAC.

Responsibilities related to converging technologies are provided below.

<b>Converging Technologies Responsibilities</b>
<p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that nontraditional IT components connected to sensitive systems meet the security requirements detailed in this handbook and are certified and accredited for that purpose.</li> <li>• Ensure media storage devices included in copiers, fax machines, printers, etc., are properly sanitized before leaving DHS control.</li> <li>• Ensure audit logs are maintained and reviewed for nontraditional IT components that store or process sensitive information.</li> </ul> <p><b>Network/System Administrators</b></p> <ul style="list-style-type: none"> <li>• Protect and monitor network connections to nontraditional IT devices such as fax machines and copiers.</li> </ul> <p><b>Facility Managers</b></p> <ul style="list-style-type: none"> <li>• Notify and coordinate with the ISSO when facility systems (e.g., HVAC and alarm systems) require connectivity to sensitive systems.</li> <li>• Ensure proper physical security is afforded to infrastructure equipment that processes, stores, or connects to a sensitive system.</li> </ul>








The use of nontraditional IT components without appropriate safeguards presents risks to DHS organizations in part because these devices are typically not thought of as IT systems.

Wireless devices must be secured as specified in Section 4.6, Wireless Communications.

Copiers with the capability to process sensitive documents must be secured in the same manner as facsimile machines (see Section 4.5.2). Sanitization of media included in high-end copiers (or other devices) must be carried out in the manner prescribed in Section 4.3.3, Media Sanitization and Disposal. If the device is a multifunction device, the facsimile functions must be secured in the same manner as stand-alone facsimile machines. Printing functions must be secured in accordance with the provisions in Section 4.3.4, Production, Input/Output Controls.

HVAC, fire suppression, and power equipment (including emergency power backup) are to be secured in accordance with the requirements specified for PBXs, as described in Section 4.4.1. If these do not have internal auditing functions, manual audit/access logs are to be maintained by a trusted employee who accompanies any individual who performs maintenance, upgrade or repair on the indicated systems.

The devices discussed in this section that have the capability to process or store sensitive data, whether or not such devices are connected to DHS networks, shall be clearly documented in the Security Plan and certified and accredited for that functionality. The risks of using such devices shall be identified along with countermeasures employed to mitigate these risks. This information shall also be included in applicable rules of behavior and addressed in awareness training orientation and refresher sessions.

## 5.0 TECHNICAL CONTROLS

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

Technical controls focus on security controls that a computer system executes. These controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

### 5.1 Identification and Authentication

**Identification** is the process of telling a system the identity of a subject. Usually this is done by entering a name or presenting a token to the system via a smart card. The identity of each user must be established prior to authorizing access to the system, and each system user must have his or her own unique User ID.

**Authentication** is the process of proving that a subject is who the subject claims to be. Authentication is a measure used to verify the eligibility of a subject and the ability of that subject to access certain information. There are three ways of authenticating oneself:

- Something you know (e.g., password)
- Something you have (e.g., a smart card)
- Something you are (e.g., a biometric such as a fingerprint)

DHS systems must be designed to ensure that each user is authenticated before access is permitted. Concurrent logins to the same system or application using the same authentication credentials are not allowed, unless a specific business or operational need is documented and approved by the DAA.

<b>DHS Policy</b>
<b>a.</b> Components shall ensure that user access is controlled and limited based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.
<b>b.</b> For IT systems requiring authentication controls, the IT system shall ensure that each user is authenticated before IT system access occurs.
<b>c.</b> 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.
<b>d.</b> 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.
<b>e.</b> All user authentication materials shall be treated as sensitive material and shall carry a level as high

<b>DHS Policy</b>
-------------------

as the most sensitive data to which that user is granted access using that authenticator.
---

Identification and authentication responsibilities are provided below.

<b>Identification and Authentication Responsibilities</b>
---

**CISO**

- Establishes and enforces identification and authentication policy.
- Provides technical expertise and evaluates the effectiveness of identification and authentication approaches.
- Assesses technology opportunities that have the potential to enhance compliance with identification and authentication requirements.

**Certifying Officials**

- Ensure that systems limit user access based on the identification and authentication of each user prior to certifying the system.

**System Owners/IT Project Managers**

- Ensure adequate resources are budgeted for information assurance; assess identification and authentication technology opportunities for potential application to DHS systems.

**System/Network Administrators**

- Ensure that the system identifies every user as unique.
- Secure and administer privileged accounts using authentication technology stronger than passwords.

**ISSOs**

- Brief users on identification and authentication procedures and protection requirements.
- Monitor/enforce compliance with identification and authentication requirements.
- Perform system audits to verify compliance.

**Users**

- Comply with identification and authentication guidance, specifically guidance pertaining to password management (see Section 5.1.1.1).
- Report violators of security policies.

### 5.1.1 Passwords

The least expensive method for authenticating users is a password system in which authentication is performed each time a password is used. More sophisticated authentication techniques, such as smart cards and biological recognition systems (e.g., retina scanner, handprint, voice recognition), shall be cost-justified through the risk assessment process.

A password is a sequence of characters used for authentication purposes. Passwords are often used to authenticate the identity of a system user and, in some instances, to grant or deny access to private or shared data. Passwords are important because they are often the first line of defense against hackers or insiders who may be trying to obtain unauthorized access to a computer system. Passwords provide a reasonable degree of authentication that the entity is the authorized

user of the User ID, username, or logon ID. They are one of the most common methods used for controlling system access. To be used effectively, strong password policies must be implemented, and users and system administrators must follow the DHS password guidelines.

<b>DHS Policy</b>
<b>a.</b> In those systems where user identity is authenticated by password, the system ISSO shall determine and enforce appropriate measures to ensure that strong passwords are used.
<b>b.</b> The ISSO shall determine and enforce the appropriate frequency for changing passwords but in no case shall the frequency be less often than every 180 days.
<b>c.</b> DHS users shall not share personal passwords.
<b>d.</b> Use of group passwords is limited to situations dictated by operational necessity or critical for mission accomplishment. Use of a group User ID and password must be approved by the appropriate DAA.
<b>e.</b> Scripted passwords shall not be used.

The use of a personal password by more than one individual is prohibited throughout the DHS. However, it is recognized that, in certain circumstances such as the operation of crisis management or operations centers, watch team and other duty personnel may require the use of group User IDs and passwords.

#### 5.1.1.1 Selecting Strong Passwords

Users must select well-constructed passwords. When selecting a password, use the following DHS password guidelines to ensure that the password chosen is in compliance with DHS requirements. For guidance on how to change passwords for a variety of DHS systems, see DHS 4300A Attachment L, *Password Management*.

<b>Required Action</b>	<b>Benefit Gained</b>
Passwords shall— <ul style="list-style-type: none"> <li>• Be at least 8 characters in length.</li> <li>• Contain a combination of alphabetic, numeric, and special characters.</li> <li>• Not be the same as the previous 8 passwords</li> </ul>	These requirements make it more difficult for a password guesser to obtain passwords. They increase the set of combinations that must be guessed and provide a mixture to defeat a dictionary attack.
Passwords shall not contain any dictionary word.	Prevents dictionary type of attacks.

Required Action	Benefit Gained
Passwords shall not contain any proper noun or the name of any person, pet, child, or fictional character. Passwords shall not contain any employee serial number, Social Security number, birth date, phone number, or any information that could be readily guessed about the creator of the password.	Helps prevent a password guess based on a hacker's personal knowledge of the user.
Passwords shall not contain any simple pattern of letters or numbers, such as "qwerty" or "xyz123".	Protects against dictionary attacks
Passwords shall not be any word, noun, or name spelled backwards or appended with a single digit or with a two-digit "year" string, such as 98xyz123.	Protects against dictionary attacks
Pass phrases, if used in addition to or instead of passwords, should follow the same guidelines.	Consistent application of guidelines.
Passwords shall not be the same as the User ID.	Risk of unauthorized access is reduced, as hackers initially try "obvious" passwords such as username and User ID.

### 5.1.1.2 Results of Weak Passwords

Weak passwords can allow internal users and external hackers, who achieve access to the internal network, to gain greater access to DHS systems. Because hackers and other unauthorized users know that passwords are the key to gaining access to systems, there have been a variety of methods and tools that have been created to crack passwords, including guessing.

Hackers have access to a variety of password-cracking tools. While tools provide a means for hackers to obtain passwords, often password information is given directly to hackers. For example, a hacker may be able to disguise himself as an authorized user and call the user's system administrator or help desk and ask that a password be reset. If the system administrator and/or help desk staff has not implemented stringent user identification controls, it would be very easy for a hacker to gain access to an authorized user account with the new password. As a result, the authorized user will be locked out of his or her own system because the hacker had the password changed.

Brute force attacks involve manual or automated attempts to guess valid passwords. Simple password-guessing programs can be easily created and there are numerous password-guessing programs available on the Internet. Most hackers have a "password hit list," which is a collection of default passwords automatically assigned to various system accounts whenever they are installed. For example, the default password for the guest account in most UNIX systems is "guest."

Many hackers will try to guess passwords using personal information of a user, such as the birth date, name of spouse/children, pets, employee ID number, etc. Often, hackers will practice what

they call “social engineering,” which involves talking with employees to find out things about the systems in their office, and, more importantly, personal information that will help them guess passwords.

Users tend to choose passwords that are easy to remember such as the name of a family member or pet, a birth date, or a word that may mean something to the user. Unfortunately, these types of passwords are the easiest for others to guess.

*People are the key to constructing good passwords.* Poorly constructed passwords make it much easier and faster for someone to find out a password. The longer it takes hackers to get a password, the more likely they are to move onto other methods of gaining access to the system.

It should be noted that many computer systems use auditing features that keep a record of actions initiated by the users while on the system. Thus, once a hacker cracks a password and gains access to the system using the appropriate User ID, the system audit logs will record that the User ID was used in taking harmful actions on the system. Authentication is the basis for control and accountability of the users on the system.

### 5.1.1.3 System Administrator Responsibilities

A secure method for initial distribution of passwords is for the user to appear at the terminal of the administrator or for help desk personnel to appear at the user’s computer and authenticate by whatever means humans use to authenticate (e.g., driver’s license, student ID, birth certificate, major credit cards, etc.). The administrator can create the account and an initial strong password (randomly chosen from a large space), give it to the user, and instruct the user to use the password only for an initial login and then change the password, using the DHS password guidelines.

As a system administrator, it is important that the following DHS password guidelines be used to ensure that password policies and settings are in compliance with DHS requirements.

Required Action	Benefit Gained
Do not store passwords in a clear text file.	Avoids situation where convenience and speedy login are achieved at the expense of security.
Passwords shall be changed or expire in 180 days or less.	Reduces the likelihood of unauthorized penetration by limiting password life.
Do not enable a password to be reused for at least 8 iterations.	Reduces the likelihood of unauthorized penetrations by increasing password variability.
Allow only one user per account; never share User IDs or passwords.	Provides user accountability.
Never assign a login account a password that is the same string as the User ID or that contains the User ID.	Eliminates the hackers’ first line of attack, which is to try User ID as the password once they get a telnet prompt.
Never install a guest/guest account.	Prevents penetration via certain well-known vulnerabilities in some User Datagram Protocol (UDP) services.

Required Action	Benefit Gained
Deactivate unused accounts monthly. For systems with a low impact for the confidentiality security objective, consider an account unused if no login has occurred in 90 days. For systems with a moderate or high impact for the confidentiality security objective, consider an account unused if no login has occurred in 30 days.	Prevents a formerly authorized user from continuing to use the host.
No accounts will be named anonymous, ftp, telnet, www, host, user, bin, nobody, etc.	Avoids accounts commonly attacked via the password-guessing method: e.g., ftp/ftp.
The manager or owner of the host shall revalidate all User IDs at least annually.	Best security practice to clean out User IDs of ex-employees and to verify which User IDs are valid.
Never set any password equal to the null string, which is equivalent to no password at all.	Follows best security practices.

Privileged accounts are to be secured by authentication technology stronger than that based only on a User ID and password. All actions taken by privileged users with respect to systems and applications should be encrypted to prevent “playback” attacks; they must also be logged for auditing purposes. All passwords, algorithms, keys, certificates, codes, or other schemes that are used by the system for authentication purposes must be stored in a manner that prevents unauthorized individuals from gaining access to them. A system can be compromised without proper, secure storage.

## 5.2 Access Control

Users are responsible for protecting all DHS information to which they are granted access. Access controls restrict access to system objects such as files, directories, and devices based upon the identity of the user, or the group to which the user belongs. The purpose of access controls is to protect against the unauthorized disclosure, modification, or destruction of the data residing in these systems, as well as the applications themselves. Automated systems are vulnerable to fraudulent or malicious activity by individuals who have the authority or capability to access information not required to perform their job-related duties. Access control policy is designed to reduce the risk of an individual acting alone from engaging in such fraudulent or malicious behavior. The Principle of Least Privilege states that users should only be able to access the system resources needed to fulfill the user’s job responsibilities.

**Principle of Least Privilege:** Requires that each user in a system be granted the most restrictive set of privileges (or lowest clearance) needed for performance of authorized tasks. The application of this principle *limits the damage that can result from an accident, error, or unauthorized use.*

### DHS Policy

- a. Components shall implement access control measures that provide protection from unauthorized

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

Access control responsibilities are provided below.

<b>Access Control Responsibilities</b>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Establish and enforce access control policy.</li> <li>• Provide technical expertise and evaluate the effectiveness of access control approaches.</li> </ul> <p><b>Certifying Officials</b></p> <ul style="list-style-type: none"> <li>• Certify that adequate access controls are in place.</li> </ul> <p><b>System/Network Administrators</b></p> <ul style="list-style-type: none"> <li>• Ensure that access controls are in place and functioning as intended.</li> <li>• Ensure that access controls provide the security features outlined in this document.</li> <li>• Ensure that systems prevent users from having multiple concurrent active sessions for one identification unless the DAA has granted authority based upon operational business needs.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that access controls are in place and functioning as intended.</li> <li>• Ensure that access controls provide the security features outlined in this document.</li> </ul>

Network/system administrators and ISSOs are responsible for ensuring that access controls are in place and operating as intended. It is especially critical that the authority to add, change, or remove component devices, dial-up connections, and network addresses and protocols, or to remove or alter programs be tightly controlled with access limited to only a select group of authorized personnel.

- **Initial User Access**

Users who need access to DHS systems and networks must have completed a background investigation prior to being granted access. The user's supervisor or project manager must also determine the systems the user needs to access and the levels of access the user needs to do his or her job. User access will vary depending on the position the user holds. The system owner or designated representative must approve user access privileges.

- **Review of Access Privileges**

The data a user needs to access will change over time. Therefore, supervisors have the responsibility to ensure that access control lists are current and up-to-date. This requirement

also applies to contractors and other non-DHS personnel with access to any DHS systems. ISSOs have an oversight responsibility to ensure this is being accomplished. These actions are reviewed as part of the C&A process and during annual self-assessments.

Access control policies and procedures need to be written down and stored in an off-site location. They need to be accessible in the event of an emergency. This information also needs to be included in the Contingency Plan.

- **Terminated and Departing Employees**

System/LAN administrators and ISSOs must ensure that all departing employees have their access privileges terminated immediately. No former employee should have any ability to access system resources after their term of employment has ended. Procedures vary depending on whether the separation is voluntary or involuntary. Termination of access privileges also applies to employees whose job functions have changed such that they no longer require access to the level of sensitive information to which they were previously granted. See Section 4.1.6, Separation from Duty, for detailed guidance on this subject.

- **Secure Remote Access**

Hardware security tokens, such as cryptographic smartcards, can be issued to DHS employees and contractors who have a valid need to remotely access DHS systems and data.

### 5.2.1 Automatic Account Lockout

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

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

Automatic account lockout responsibilities are provided below.

<b>Automatic Account Lockout Responsibilities</b>
<p><b>CISO</b></p> <ul style="list-style-type: none"> <li>• Establishes and enforces automatic account lockout policies.</li> </ul>
<p><b>System/Network Administrators</b></p> <ul style="list-style-type: none"> <li>• Ensure that systems are configured to lock a user's account for 20 minutes after 3 unsuccessful logon attempts.</li> </ul>
<p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that systems are configured to lock a user's account for 20 minutes after 3 unsuccessful</li> </ul>

<b>Automatic Account Lockout Responsibilities</b>
logon attempts.

### 5.2.2 Automatic Session Termination

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

Components may establish a more stringent automatic session lockout policy than the DHS 20-minute limit. The user will need to log on again in order to activate the session.

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

Automatic session lockout responsibilities are provided below.

<b>Automatic Session Lockout Responsibilities</b>
<p><b>CISO</b></p> <ul style="list-style-type: none"> <li>Establishes and enforces automatic session lockout policies.</li> </ul> <p><b>System/Network Administrators</b></p> <ul style="list-style-type: none"> <li>Ensure that systems are configured to terminate any user session that has remained idle for 20 minutes.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>Ensure that systems are configured to terminate any user session that has remained idle for 20 minutes.</li> </ul>

### 5.2.3 Warning Banner

The CISO stipulates that the following banner statement be displayed on all DHS IT systems during logon:

You are about to access a Department of Homeland Security (DHS) computer system. This DHS computer system and the data therein are property of the U.S. Government and provided for official U.S. Government information and use. Access to this system is restricted to authorized users only. Unauthorized access, use, or modification of this computer system or of the data contained herein, or in transit to/from this system, may constitute a violation of section 1030 of title 18 of the U.S. Code and other federal or state criminal laws. Anyone who accesses a Federal computer system without authorization or exceeds his or her access authority, or obtains, alters, damages, destroys, or discloses information, or prevents authorized use of information on the computer system, may be subject to administrative penalties, fines or imprisonment.

This DHS computer system and any related equipment is subject to monitoring for administrative oversight, law enforcement, criminal investigative purposes, inquiries into alleged wrongdoing or misuse, and to ensure proper performance of applicable security features and procedures. As part of this monitoring, DHS may acquire, access, retain, intercept, capture, retrieve, record, read, inspect, analyze, audit, copy and disclose any information processed, transmitted, received, communicated, and stored within the computer system. If monitoring reveals possible misuse or criminal activity, notice of such may be provided to appropriate supervisory personnel and law enforcement officials. DHS may conduct these activities in any manner without further notice.

Accordingly, there can be no expectation of privacy in the course of your use of this computer system. The use of a password or any other security measure does not establish an expectation of privacy. There is no expectation of privacy in any media, peripherals or other devices placed in or connected to the computer system.

By clicking “I agree” below or by using this system, you consent to the terms set forth in this notice.

You may not process classified national security information on this computer system.

The use of the warning banner serves as a reminder to all users that the computers they are accessing are Government computers and must be used in accordance with good security practices.

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

Warning banner responsibilities are provided below.

<b>Warning Banner Responsibilities</b>
<b>CISO</b>
<ul style="list-style-type: none"> <li>• Establishes and enforces the use of appropriate standard Warning Banner for all internal DHS IT systems.</li> <li>• Establishes and enforces the use of a standard Warning Banner and Privacy Statement for display at all publicly accessible entry points to DHS IT systems.</li> </ul>
<b>System/Network Administrators</b>
<ul style="list-style-type: none"> <li>• Ensure that internal IT systems under their controls are configured to display the approved</li> </ul>

<b>Warning Banner Responsibilities</b>
<p>Department Warning Banner.</p> <ul style="list-style-type: none"> <li>• Ensure publicly accessible IT systems under their control are configured to display the approved Department Warning Banner and Privacy Statement.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that internal IT systems under their controls are configured to display the approved Department Warning Banner.</li> <li>• Ensure publicly accessible IT systems under their control are configured to display the approved Department Warning Banner and Privacy Statement.</li> </ul>

### 5.3 Auditing

A fundamental computer security principle is that each person is to be individually accountable for his or her actions while using the system. By providing the ability to track a user's activities while accessing an automated system, auditing tools are an effective method of enforcing this principle. Audit trails maintain a record of system activity by both system or application processes as well as by individual user activity. In conjunction with appropriate tools and procedures, auditing can further several security-related objectives including:

- Individual accountability
- Reconstruction of events
- Intrusion detection
- Problem identification

Specifically, audit trails can track the identity of each subject attempting to access the system, the time and date of access, and the time of log off. In addition, audit trails can capture all activities performed during a session and can specifically identify those activities that have the potential to modify, bypass, or negate the system's security safeguards. The auditing technique used must be able to support after-the-fact investigations of how, when, and why normal operations ceased.

<b>DHS Policy</b>
<p><b>a.</b> Audit records shall be sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. Audit records shall be reviewed as specified in the IT System Security Plan. The audit record shall contain at least the following information:</p> <ul style="list-style-type: none"> <li>– Identity of each user and device accessing or attempting to access an IT system</li> <li>– Time and date of the access and the logoff</li> <li>– Activities that might modify, bypass, or negate IT security safeguards</li> <li>– Security-relevant actions associated with processing</li> <li>– All activities performed using an administrator's identity</li> </ul>
<p><b>b.</b> Audit records for financial systems or for systems hosting or processing PII shall be reviewed by the system administrator monthly. Unusual activity shall be reported to the system owner and ISSM.</p>

<b>DHS Policy</b>
<b>c.</b> Components shall ensure that their audit records and audit logs are protected from unauthorized modification, access, or destruction.
<b>d.</b> Components shall ensure that audit logs are recorded and retained in accordance with the Component's Record Schedule or the DHS Records Schedule. At a minimum audit trail records shall be maintained online for at least 90 days.
<b>e.</b> Components shall evaluate the system risks associated with extracts of PII from databases. If the risk is determined to be sufficiently high, a procedure shall be developed for logging computer-readable data extracts. If logging these extracts is not possible, this determination shall be documented, and compensating controls identified in the SSP.
<b>f.</b> Computer-readable data extracts involving PII shall be erased within 90 days unless the information included in the extracts is required beyond the 90 days. Erasure of the extracts or the need for continued use of the data shall be documented by the Component Privacy Officer or PPOC.

Auditing responsibilities are provided below.

<b>Auditing Responsibilities</b>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Ensure that all DHS IT systems maintain an audit record sufficient to reconstruct security relevant events.</li> <li>• Evaluate auditing requirements at the DHS Component level; budget for and select appropriate auditing tools.</li> <li>• Establish policy for retention of audit logs.</li> <li>• Ensure auditing is performed independently of system/network administration.</li> </ul> <p><b>System Owners</b></p> <ul style="list-style-type: none"> <li>• Ensure adequate resources are budgeted for implementing and maintaining an effective auditing capability.</li> <li>• Work with IT managers to identify critical functions to be subjected to auditing and keep apprised of auditing findings.</li> <li>• Ensure auditing is performed independently of system/network administration.</li> </ul> <p><b>System/Network Administrators</b></p> <ul style="list-style-type: none"> <li>• Maintain an audit record sufficient to reconstruct security relevant events.</li> <li>• Ensure that the audit record includes: <ul style="list-style-type: none"> <li>– The identity of each person and device accessing or attempting to access the system.</li> <li>– The time and date of the access and when the user logged off.</li> <li>– Activities performed using an administrator's identification.</li> <li>– Activities that could modify, bypass, or negate the system's security.</li> <li>– Sufficient detail to facilitate reconstruction if compromise or malfunction occurs.</li> <li>– Security-relevant actions associated with processing.</li> </ul> </li> </ul>

<b>Auditing Responsibilities</b>
<ul style="list-style-type: none"> <li>• Protect audit records against unauthorized access, modification, or destruction.</li> <li>• Retain audit records for a minimum of 90 days or in accordance with the Security Plan and ensure that audit records are regularly backed up.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that the Security Plan addresses accountability and auditing.</li> <li>• Ensure that the risk analysis documents the rationale and justification for any DHS IT system that does not implement an auditing capability.</li> <li>• Ensure that audit records include all required elements.</li> <li>• Review audit records at least once per week or in accordance with the Security Plan.</li> <li>• Ensure that audit collection and review procedures contain adequate separation of duties provisions.</li> <li>• Report security-relevant events to the Component CSIRC.</li> </ul>






Audit trail records must be maintained online for at least 90 days, thereby allowing rapid access to recent information. Audit trails should be preserved for a period of seven years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease. Preservation of the audit information should be part of the IT Contingency and business continuity plans, so that events preceding a disaster or interruption of service can be reconstructed.

The need to review the information captured by the auditing process is of paramount importance. To be effective, audit trails must be periodically reviewed and analyzed. In many cases, it is only through the review process that incidents of unauthorized access, modification, or destruction are uncovered. Audit trails also need to be secured to prevent tampering and backed up regularly.

## **5.4 Network and Communications Security**

This section addresses vulnerabilities inherent in network security and the technical controls needed to mitigate the risks associated with these vulnerabilities. Network security encompasses remote access, network monitoring, external connections, boundary protection, Internet usage, email security, and vulnerability scanning.

### **5.4.1 Remote Access and Dial-In**

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

Note: Remote access solutions that do not comply with the requirements of FIPS 140-2 are not authorized.

<b>DHS Policy</b>
<p><b>a.</b> Data communication connections via modems shall be limited and shall be tightly controlled as</p>

<b>DHS Policy</b>
such connections can be used to circumvent security controls intended to protect DHS networks. Data communication connections are not allowed unless they have been authorized by the Component ISSM.
<b>b.</b> Components shall ensure that remote access and approved dial-in capabilities provide strong authentication and access control and audit and protect sensitive information throughout transmission. In addition, remote access solutions shall comply with the encryption requirements of FIPS 140-2, <i>Security Requirements for Cryptographic Modules</i> . Dial-up connections shall be centrally managed by each Component to ensure integrity of network security. Strong authentication for remote access should consider two-factor authentication.
<b>c.</b> The Risk Assessment and SSP shall document any remote access of PII, and the remote access shall be approved by the DAA prior to implementation.
<b>d.</b> Remote access of PII shall comply with all DHS requirements for sensitive systems, including strong authentication. Strong authentication shall be accomplished via virtual private network (VPN) or equivalent encryption and two-factor authentication. Any two-factor authentication shall be based on agency-controlled certificates or hardware tokens issued directly to each authorized user.
<b>e.</b> Remote access of PII shall not permit the download and remote storage of information unless the requirements for the use of removable media with sensitive information have been addressed. All downloads shall follow the concept of least privilege and shall be documented with the SSP.

Remote access and dial-in responsibilities are provided below.

<b>Remote Access and Dial-In Responsibilities</b>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Establish and enforce remote access control policy for each Component.</li> <li>• Provide technical expertise and evaluate the effectiveness of remote access control approaches.</li> </ul> <p><b>System/Network Administrators</b></p> <ul style="list-style-type: none"> <li>• Ensure that remote access controls are in place and functioning as intended.</li> <li>• Ensure that remote access controls provide strong identification and authentication.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure that remote access controls are in place and functioning as intended.</li> <li>• Ensure that remote access controls provide the security features outlined in this document.</li> </ul> <p><b>Users</b></p> <ul style="list-style-type: none"> <li>• When remotely accessing DHS systems, ensure that the equipment used to gain access is protected from viruses and other malicious code and that the protection software is kept current.</li> </ul>

Unauthorized access is the biggest risk associated with remote access facilities. If untrusted or uncleared persons obtain unauthorized access, they can violate the integrity, confidentiality, and availability standards of the Department. An unsecured modem or other dial-in facility could provide a backdoor for unauthorized users (inside or outside of the DHS) to the entire DHS network. Malicious individuals can exploit improperly configured remote control software.

There are commercially available products that can be used in conjunction with other network protection mechanisms to reduce the risks of unauthorized access. These require the use of authentication methods stronger than passwords and user IDs.

Components must develop and implement acquisition procedures to ensure that only approved hardware and software products can be purchased and operated without the need for additional approval of their respective architecture review function.

#### 5.4.2 Network Security Monitoring

Security monitoring, detection and analysis are key functions and are critical to maintaining the security of DHS information systems. Monitoring and analysis is limited to observing network activity for anomalies, malicious activities and threat profiles. Content analysis is not within the scope of network monitoring.

Component CSIRCs lead the effort in monitoring network security. ISSMs, ISSOs, and system/network administrators respond to and participate in intrusion alerts and CSIRC-led incident response investigations. They also evaluate the impact of each event on the system and implement any necessary corrections.

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

Network security monitoring responsibilities are provided below.

<b>Network Security Monitoring Responsibilities</b>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Establish policy and implement and manage a viable intrusion detection program within each Component.</li> <li>• Provide guidance, as needed, when responding to intrusion alerts from the SOC.</li> </ul> <p><b>SOC</b></p> <ul style="list-style-type: none"> <li>• Monitor DHS systems and networks using various network security technologies.</li> <li>• Initiate computer security incident procedures when incidents are discovered.</li> </ul> <p><b>ISSOs/System Administrators</b></p> <ul style="list-style-type: none"> <li>• Respond to intrusion alerts when notified by SOC/.</li> <li>• Participate in SOC-led incident response investigations.</li> <li>• Evaluate the impact of the event on the system.</li> <li>• Implement necessary corrections.</li> </ul>

### **5.4.2.1 What Is Intrusion Detection?**

Intrusion detection is the art of detecting inappropriate, incorrect, or malicious activity. Systems that operate on a host to detect malicious activity on that host are called host-based intrusion detection systems (HIDS). Those that operate on a network are referred to as network intrusion detection systems (NIDS). Intrusion detection is viewed as an integral part of a layered security model.

Intrusion detection operates on the principle that any attempt to penetrate a system can be detected in real time as opposed to actually stopping the penetration, as is the case with firewalls. This principle is based on the assumption that it is virtually impossible to close every potential security breach. NIDS are designed to identify break-in attempts and stop them, in some cases working in conjunction with firewalls to alter the access control lists to halt an incursion. HIDS can offer the equivalent of a software firewall installed on the host, stopping or preventing would-be intruders.

Intrusion prevention systems (IPSs) are closely related to IDSs. Some IDS technologies currently provide intrusion protection by halting malicious data transmissions and disconnecting communication from the host from which they originate. Others take the additional step of reconfiguring firewalls to permanently block attacking hosts from sending data into the network.

Firewalls are designed to prevent unauthorized entry, but firewalls can fail or be compromised by an intruder. Intrusion detection systems supplement firewalls by alerting the organization that an attack may have occurred or be occurring. Firewalls are also incapable of protecting a network from internal compromise, but IDSs can alert network and system managers of such an attack.

### **5.4.2.2 Methods and Techniques**

The most common approaches to intrusion detection are statistical anomaly detection and pattern matching (signature) detection. Statistical anomaly involves tracking system use and establishing a baseline of what is “normal” and setting an acceptable range of parameters to which the system normally adheres. When the system goes beyond the statistical ranges, an intrusion may have occurred and an alarm is given. Pattern matching is simply what its name implies. Patterns of known attacks are part of the IDS database. Attack patterns for denial of service attacks, buffer overflow attacks, and backdoors are well known. These are known as signatures. When these signatures are detected, an alarm is given. When alarms are given, those monitoring the IDS investigate to determine if an intrusion has in fact occurred and react accordingly. Event correlation systems can compare information from various security devices and reduce the likelihood of unnecessary response to “false positives,” which may arise from an attack signature matching allowed activities. Such systems can also reduce the likelihood that the monitoring staff is distracted from noticing an actual attack by a flurry of alarms raised by relatively innocuous activities.

### **5.4.2.3 Monitoring**

The DHS Computer Security Incident Response Center (CSIRC) will accomplish the monitoring of DHS systems and networks. Upon receipt of an alarm, operators will investigate to determine the validity of the alarm. Once confirmed, the operator will notify the ISSO and/or the system

administrator for corrective action. If the problem is deemed critical, senior management will be notified and involved to determine the appropriate course of action.

### 5.4.3 Network Connectivity

A number of management, operational, and technical controls impact network connectivity. These include identification and authentication controls, audit logging, integrity controls, and periodic reviews of programs/systems to ascertain whether or not changes that could adversely affect security have occurred.

<b>DHS Policy</b>
<b>a.</b> Components shall ensure that appropriate identification and authentication controls, audit logging, and access controls are implemented on every network component.
<b>b.</b> Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or interconnect service agreements.
<b>c.</b> Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA). Interconnections between DHS Components shall require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. ISAs shall be signed by both DAAs or by the official designated by the DAA to have signatory authority.
<b>d.</b> ISAs shall be reissued every three years or whenever any significant changes have been made to any of the interconnected systems.
<b>e.</b> ISAs shall be reviewed as a part of the annual FISMA self-assessment.

Network connectivity responsibilities are provided below.

<b>Network Connectivity Responsibilities</b>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Provide guidance and enforce management, operational, and technical controls that apply to network and system security configuration and monitoring.</li> <li>• Evaluate the risks associated with external connections.</li> <li>• Review programs/systems periodically to ascertain if changes have occurred that could adversely affect security.</li> </ul> <p><b>DAAs or Designated Official</b></p> <ul style="list-style-type: none"> <li>• Review, approve, and sign the Interconnection Security Agreement (ISA).</li> <li>• Ensure that ISAs are reissued every three years or whenever significant changes are made to any of the interconnected systems.</li> </ul> <p><b>System Owners</b></p> <ul style="list-style-type: none"> <li>• Establish the requirement for the external connection and assess the associated risks.</li> </ul>

<b>Network Connectivity Responsibilities</b>
<p><b>Network Administrators</b></p> <ul style="list-style-type: none"> <li>• Ensure technical controls governing use of the external connection remain in place and function properly.</li> <li>• Assist in development of the ISA.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Coordinate with the external agency in development of the ISA.</li> <li>• Assist in preparation of the ISA and ensure all external connections are documented in the System Security Plan, Risk Assessment, and security operating procedures.</li> <li>• Review ISAs as a part of the annual FISMA self-assessment.</li> <li>• Monitor compliance.</li> </ul> <p><b>Users</b></p> <ul style="list-style-type: none"> <li>• When connecting to DHS networks, ensure the equipment used to access these networks is protected from viruses and other malicious code and the protection software is kept current.</li> </ul>








### 5.4.3.1 Interconnection Security Agreements

Proper management of network connections is vital to ensuring the confidentiality, integrity, and availability of the data processed by a system. Interconnections of systems must be established in accordance with NIST SP 800-47 (*Security Guide for Interconnecting Information Technology Systems*). An interconnection security agreement (ISA) is required whenever the security policies of the interconnected systems are not identical and the systems are not administered by the same entity/DAA. The ISA documents the security protections on the interconnected systems to ensure only acceptable transactions are permitted. ISAs must be reissued every three years or whenever significant changes have been made to any of the interconnected systems. Component personnel must review ISAs as part of the annual FISMA self-assessment.

All external connections must be identified and documented in the System Security Plan, the risk assessment, and other C&A documentation as necessary. The risk associated with these connections must be addressed during the C&A process.

An ISA should address the following areas:

- **Purpose:** This section should explain the rationale for the interconnection and contain a one- or two-paragraph statement that justifies the need to interconnect the two systems.
- **Interconnection Statement of Requirements:** This section documents the formal requirement for connecting the two systems. The following items should be addressed in this section:
  - The requirement for the interconnection, including the benefits derived
  - The names of the systems being interconnected
  - The type of connection (Frame Relay, T1, etc.)
  - Physical location of connection equipment, including addresses and room numbers
  - Primary Points of Contact (POC) for both systems

- The agency name(s) or organization that initiated the requirement
- **System Security Considerations:** This section documents the security features in place to protect the confidentiality, integrity, and availability of the data and the systems being interconnected. This includes such areas as incident reporting and personnel clearances. Technical representatives from each organization need to discuss the contents of this section and come to a mutual agreement as to which items are to be included.
- **Topological Drawing:** Each ISA must include a topological drawing depicting the end-to-end interconnectivity in a clear and readable manner. The drawing should include:
  - All data communications paths (not program system paths), circuits, etc., used for the interconnection beginning with the DHS-owned system(s) traversing through all interconnected systems to the non-DHS end-point
  - The logical location of all components (mainframe computers, host processors, hubs, firewalls, encryption devices, routers, frame relay devices, secure frame units [SFU], communications service units [CSU], data service units [DSU], and customer personal computers).
- **Signatures and Comments:** Each ISA must be signed by the Designated Accrediting Authority (DAA) of each connecting system and/or organization or by the official designated by the DAA to have signatory authority for ISAs. This section acknowledges that the ISA is subject to change, will be reviewed annually, and will be modified as circumstances warrant. This section must include a statement that the ISA may not be unilaterally modified and that any changes must be reviewed and jointly agreed upon.

Details on completing an ISA are contained in DHS 4300A Attachment N, *Preparation of Interconnection Security Agreements*.

#### 5.4.4 Firewalls

Within the DHS, boundary protection of IT resources is accomplished by the installation and operation of firewall systems. Firewalls, when used in concert with a variety of additional security controls such as intrusion detection systems, personnel background checks, security guards, data encryption, and physical security barriers, provide an added level of assurance that unauthorized personnel will be unable to access the Department's automated systems.

By tracking and controlling data, and deciding whether or not to pass, drop, reject, or encrypt the data, firewalls have proven to be an effective means of securing a network.

<b>DHS Policy</b>
<b>a.</b> Components shall restrict physical access to firewalls to authorized personnel.
<b>b.</b> Components shall implement strong identification and authentication for administration of the firewalls.
<b>c.</b> Components shall encrypt remote maintenance paths to the firewalls.
<b>d.</b> Components shall conduct quarterly testing to ensure that firewall configurations are correct.

<b>DHS Policy</b>
<p>e. Component SOCs shall ensure reports on security operations status and incident reporting are provided to the CISO Security Operations Program Director as required.</p>

Responsibility for the future deployment and management of firewalls will be determined at a later date. General responsibilities are included below.

<b>Firewall Responsibilities</b>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Develop procedures and schedules for deploying firewall systems.</li> </ul> <p><b>ISSOs and ADP Support Personnel</b></p> <ul style="list-style-type: none"> <li>• Assist Component teams in the installation of firewall systems.</li> </ul> <p><b>Site Managers</b></p> <ul style="list-style-type: none"> <li>• Ensure that the installation team receives necessary support during and after firewall installation.</li> </ul> <p><b>SOC</b></p> <ul style="list-style-type: none"> <li>• Manage firewalls in accordance with DHS firewall policy.</li> <li>• Maintain change control over firewalls and maintain proper firewall configuration.</li> <li>• Evaluate, process, and approve changes to firewall configuration.</li> </ul>










#### 5.4.4.1 Firewall Basics

A firewall is a system or group of systems that enforce an access control policy between two networks. The actual means by which this is accomplished varies widely. Associated with the basic capabilities of access control, firewalls can authenticate the source and destination of a given data path, provide network address translation (NAT) and port address translation (PAT) and log all traffic passing through them. The logging is either done on the machine on which the firewall software runs on, or is logged to a separate machine for audit and intrusion forensic analysis.

Firewalls are often associated with filtering devices, which screen incoming (and possibly outgoing) data traffic for viruses and malware in the form of mobile code. By offloading these responsibilities to ancillary machines, the firewall can allow higher rates of data transmission.

Mobile (downloadable) code is software that is transmitted from a remote source across a network to a local system and then executed on that local system (e.g., personal computer, PDA, mobile phone, Internet appliance). Examples include ActiveX controls, Java applets, script run within the browser, and HTML email. Although mobile code is a legitimate method for distributing application software, it is most frequently associated with “malicious mobile code” (e.g., viruses, worms, Trojan horses) that executes without the permission of or any explicit action by the local system’s owner/user.

Firewalls also have two facets with respect to encryption. A frequently used mechanism is the SSHv2 protocol (Secure Shell version 2). This facility can provide for authentication by a digital certificate or a two-factor authentication mechanism, as well as strong encryption. Such a

connection should only be allowed from the protected (internal) side of a firewall, so that unauthorized outsiders are unable to affect a change.

Firewalls often have the capability to implement encrypted data communications. Although this approach might be slightly more economical, it is more prudent to have a system that functions as a firewall serve a single purpose. A separate encryption server (behind the firewall) is afforded the extra protection of being shielded by a firewall. Encryption, moreover, involves a substantial amount of computational power, which would slow down the operation of the firewall. Lastly, if the firewall system is compromised, the encryption facility is not automatically compromised at the same time.

NIST SP 800-10, *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls*, and NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*, offer guidance with respect to firewalls and the functions they can serve.

#### 5.4.4.2 Firewall Deployment

Firewall systems have been deployed to various DHS sites, and additional systems are scheduled for deployment as part of the continuing effort to provide necessary security safeguards.

Firewalls are not used solely to provide boundary protection from the outside world. In commercial environments, for example, the fiscal processing systems may be protected from the remainder of the network by firewalls. In a similar manner, the Department can use firewalls to segment systems that have various levels of sensitivity, unless they are so classified that connection to the network should be prohibited.

#### 5.4.5 Internet Security

This section provides specific DHS technical policy regarding the use and proper configuration of firewalls and the management of dial-up connections and other protocols.

DHS Policy
<b>a.</b> Any direct connection of DHS networks to the Internet or to extranets must occur through firewalls that have been certified and accredited.
<b>b.</b> Firewalls shall be configured to prohibit any protocol or service that is not explicitly permitted.
<b>c.</b> Components shall ensure that all executable code, including mobile code (e.g., ActiveX, JavaScript), is reviewed and approved by an appropriate senior official prior to the code being allowed to execute within the DHS environment. [Note: When the technology becomes available and code can be vetted for security, the policy will be “Ensure that all approved code, including mobile code (e.g., ActiveX, JavaScript), is digitally signed by the designated DHS authority and that only signed code is allowed to execute on DHS IT systems.”]
<b>d.</b> Telnet shall not be used to connect to any DHS computer. A connection protocol such as Secure Shell (SSH) that employs secure authentication (two factor, encrypted, key exchange, etc.) and is approved by the Component shall be used instead.
<b>e.</b> File Transfer Protocol (FTP) shall not be used to connect to or from any DHS computer. A connection protocol that employs secure authentication (two factor, encrypted, key exchange, etc.) and

<b>DHS Policy</b>
-------------------

is approved by the Component shall be used instead.
---

Internet security responsibilities are provided below.

<b>Internet Security Responsibilities</b>
---

**DAA**

- Ensures all external network connections are protected by a firewall and possibly other boundary protection devices that have been certified and accredited at a level commensurate with the sensitivity of the information to be protected.
- Ensures dial-up connections are addressed in the C&A documentation.

**ISSOs**

- Ensure all external network connections are addressed in the risk assessment and System Security Plan.
- Ensure all external network connections are protected by a firewall and possibly other boundary protection devices.
- Ensure all boundary protection devices are properly configured and monitored.
- Ensure dial-up connections are properly configured and secure.

**Network/System Administrators**

- Ensure all boundary protection devices are properly configured and monitored.
- Ensure firewall ports that allow file and printer sharing, whether through Microsoft NetBIOS, Common Internet File Service (CIFS), Network File Services (NFS), or TCP SMB (Server Message Block) protocols, are closed.
- Ensure firewalls are configured to prohibit any protocol or service that is not explicitly permitted.
- Ensure the following are prohibited:
  - Telnet (clear text) connections.
  - FTP unsecured (clear text) file transfers.
  - SNMP protocols that can be used to monitor and control systems
  - Cross boundary routing broadcasts
  - Address Resolution Protocol (ARP) messages
  - DNS communications across the boundary (by using split DNS with zone transfer authentication)
  - Unsecured file transfers
  - Mobile code (e.g., ActiveX, JavaScript) that has not been reviewed and digitally signed by an appropriate DHS authority.
- Ensure dial-up connections are properly configured and secure.

Sound network security practice dictates that all network connections be identified and the threats and vulnerabilities associated with these connections be analyzed. The guidance provided in Section 5.4.3, *Network Connectivity*, specifically with regard to ISAs, also applies to connections to Internet and extranet connections.

An extranet is a private network encompassing that portion of an organization's intranet that it chooses to securely share—via the Internet and the public telecommunication system—with external suppliers, vendors, or customers. An extranet requires security and privacy and may involve firewalls, digital certificates, message encryption, and virtual private networks that can tunnel through the public network.

All external connections, including extranets, must be identified and documented in the Security Plan, the Risk Assessment, and other C&A documentation as necessary. The risks associated with these connections must be addressed during the C&A process. Additionally, external network connections are to be reviewed annually by Component personnel and documented in the annual IT security assessment.

Adequate protection requires the proper selection and installation of firewalls and other boundary devices, Intrusion Detection Systems, and ancillary encryption or filtering devices. These devices must be certified and accredited prior to their use on DHS networks.

Implementation guidance for firewalls is discussed in Section 5.4.4, *Firewalls*. Intrusion Detection Systems are covered in Section 5.4.2, and encryption is addressed in Section 5.5.1. The adequacy of these devices must be monitored and reviewed as part of periodic IT security assessments.

Firewalls must be configured to prohibit any Transport Control Protocol (TCP), User Datagram Protocol (UDP) service, or other protocol that is not explicitly permitted. Of particular concern is the need to close ports that allow file and printer sharing, whether through Microsoft NetBIOS, Common Internet File Service (CIFS), Network File Services (NFS), or TCP Server Message Block (SMB) protocols. The use of file and printer sharing is associated with numerous vulnerabilities related to everything from enumeration of devices and user accounts to anonymous control of systems without authorization.

Telnet, which is prohibited on DHS systems and networks, is a utility program and protocol that allows one computer to connect to another computer on a network. After providing a username and password to login to the remote computer, a user can enter commands that will be executed as if entered directly from the remote computer. Telnet transfers all information in “clear text” (human readable text), which allows Internet service providers (ISPs) and other users on the Internet, intranet, or LAN to intercept the traffic it creates. This could allow unauthorized users to get user IDs and passwords, capture information or commands that are being sent, and potentially alter the information in the telnet connection. Telnet uses a commonly known port, which makes it easy for someone to “sniff” telnet traffic. The approved solution for this functionality is to use Secure Shell (SSH). SSH is an IETF protocol that provides encrypted connections and supports authentication with digital certificates and other secure methods of authentication.

FTP is a means of transferring files from one computer to another. FTP transfers all information in clear text (human readable text), which allows Internet Service Providers (ISPs) and other users on the Internet, intranet, or LAN to intercept the traffic it creates. This allows unauthorized users to capture information or commands and possibly alter the information in the FTP connection. FTP generally uses a commonly known port, which makes it easy for someone to “sniff” FTP traffic. The approved solution for this security risk is to use the Secure File Transfer Protocol (SFTP) component of Secure Shell (SSH). SSH is a FIPS 140-2-approved

Internet Engineering Task Force (IETF) protocol, which provides encrypted connections and supports authentication with digital certificates and other secure methods of authentication.

Use of the following is expressly prohibited:

- Telnet
- File Transfer Protocol (FTP)
- Simple Network Management Protocol (SNMP), which can be used to monitor and control systems
- Address Resolution Protocol (ARP) messages

The following have significant risks and shall be used only in conjunction with appropriate countermeasures and risk-reduction procedures:

- Cross boundary routing broadcasts
- DNS communications across the boundary (by using split DNS with authentication of zone transfers)
- Mobile code (e.g., ActiveX, JavaScript) that has not been reviewed and digitally signed by an appropriate DHS authority.

Implementation guidance for securing dial-up connections is addressed in Section 5.4.1, Remote Access and Dial-In. Dial-in connections must be strictly controlled, to the extent they can even be justified.

#### **5.4.6 Email Security**

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

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

Email is the most commonly used application for exchanging data electronically. The email process can be divided into two main components: (1) mail servers, which deliver, forward, and store mail, and (2) clients, which interface with the user and allow them to read, compose, send, and store messages.

Instant messaging (IM) and “I Seek You” (ICQ) tools provide similar capabilities to email, but are inherently less secure; the technology to secure IM and ICQ tools is still being developed. IM and ICQ tools possess all of the risks associated with unsecured email, including the capability to install software or malware on a recipient’s system without their knowledge. If IM and ICQ tools are to be used, they should not include or communicate with publicly available IM or ICQ tools provided by several Internet Service Providers. Any such tools employed need to be capable of blocking any format except pure text. This specifically includes blocking executable code, Web links, video or still images, and audio. The use of Instant Messaging and ICQ is not currently authorized for use on sensitive systems and networks.

Second only to Web servers, mail servers are the host on a network that is most often targeted by intruders. Mail servers are targeted because they communicate, to some degree, with untrusted third parties. Additionally, email has been an effective method of passing malicious code (viruses). As a result, mail servers, mail clients, and the network infrastructure that supports them must be protected. Email security issues include:

- Flaws in the email application software have been used as the means of compromising the server and subsequently the associated network.
- Denial of service (DoS) attacks may be directed to the mail server.
- Sensitive information on the mail server may be read by unauthorized individuals or changed in an unauthorized manner.
- Unencrypted sensitive information transmitted between a mail server and email client could be intercepted.
- Information within the email may be altered at some point between the sender and recipient.
- Viruses and other types of malicious code may be distributed throughout an organization via email.
- The sending of inappropriate, proprietary, or other sensitive information via email could expose an organization to legal action.

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

<b>DHS Policy</b>
-------------------

- |   |
|---|
| <ul style="list-style-type: none"> <li>– Reviewing audit logs at least weekly.</li> </ul> |
|---|

Email security responsibilities are provided below.

<b>Email Responsibilities</b>
-------------------------------

**CISO**

- Establishes Department-wide policy to secure Department email systems.

**ISSMs**

- Advise the CISO on methods for securing Department email systems.
- Enforce Department email security policies.

**Certifying Officials**

- Certify that adequate security controls are in place for email systems.

**DAA's**

- Ensure that adequate email security controls are in place prior to accreditation of the system.

**System/Network Administrators**

- Ensure email security controls are in place and functioning as intended.
- Ensure email security controls provide the security features outlined in this document.
- Test and apply patches in a timely manner.
- Remove or disable unneeded services and applications on email servers.
- Configure user authentication for email systems.
- Review and analyze log files.
- Back up data as required by the system security plan.
- Protect email systems against malicious code.
- Deploy the following network protection mechanisms:
  - Firewalls
  - Routers
  - Switches
  - Intrusion detection systems.

**ISSOs**

- Schedule semiannual/quarterly appointments with the SOC or IV&V team to scan the email system with a vulnerability assessment tool.
- Ensure that email system security controls are in place and functioning as intended.
- Ensure that email system security controls provide the security features outlined in this document and the system security plan.
- Ensure an IT Contingency Plan is in place.

Securing a mail server is a two-step process. The first step is to secure the underlying operating system. Many security issues can be avoided if the operating systems are configured

appropriately. The second step is to configure the email application. Administrators must configure their servers to apply the organization's security policy. Securing a mail server includes the following steps:

- Apply patches as they become available after first testing them in a lab environment
- Remove or disable unneeded services and applications
- Configure user authentication
- Scan the operating system with a vulnerability assessment tool

Components must consider encryption technologies to protect their email systems. Most standard mail protocols default to unencrypted user authentication and send email data in the clear. Sending data in the clear allows a hacker to compromise a user's account and/or intercept emails.

When a PKI system is properly integrated into the client email facility, it is possible to "hash" a message to determine that it has not been altered or otherwise tampered with. It is also possible to encrypt sensitive data in an email using the employee's digital certificate encryption key and digitally sign an email using the digital certificate's signing key. This establishes integrity, confidentiality, and nonrepudiation with regard to sensitive information.

The infrastructure that supports the network plays a vital role in the security of the email system. The network infrastructure is the first line of defense between the Internet and a mail server. However, network design alone cannot protect a mail server. The following steps need to be accomplished on a regular recurring basis:

- Review and analyze log files
- Back up data daily (or in accordance with the system security plan)
- Protect against malicious code (e.g., viruses, worms, Trojan horses)
- Have a recovery plan in the event of a disaster
- Test and apply patches in a timely manner
- Scan the system for vulnerabilities with a vulnerability-scanning tool

NIST SP 800-45, *Guidelines on Electronic Mail Security*, and NIST SP 800-49, *Federal S/MIME V3 Client Profile*, have valuable information detailing how to secure email. NIST 800-45 gives detailed technical guidance for Microsoft Exchange, Linux, and Unix mail services and contains general guidance on how to secure mail servers.

#### **5.4.7 Personal Email Accounts**

Just as discussing sensitive information on a cell phone in a crowd can expose the information to untrusted ears, sending sensitive email to a personal account can expose that information to a large number of unauthorized individuals.

<b>DHS Policy</b>
-------------------

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

Personal email responsibilities are provided below.

<b>Personal Email Responsibilities</b>
--

**CISO**

- Establishes DHS policy concerning the transmittal of sensitive DHS information.
- Evaluates the risks associated with the transmittal of sensitive information.

**ISSMs**

- Evaluate the risks and recommend solutions to counter the risk of transmitting sensitive DHS information.

**System Owners and Supervisors**

- Enforce DHS policy prohibiting the transmittal of sensitive DHS information to personal email accounts.

**System Administrators**

- Ensure technical controls are in place and properly functioning to prohibit and/or deter the transmission of sensitive DHS information to personal email accounts.

**ISSOs**

- Ensure technical controls are in place and properly functioning to prohibit and/or deter the transmission of sensitive DHS information to personal email accounts.
- Monitor compliance.

**Users**

- Comply with DHS policy prohibiting the transmission of sensitive DHS information to personal email accounts.

Sending email to a personal account has the following vulnerabilities:

- Because personally owned computers are not authorized for use in DHS, they are not likely to have the appropriate encryption software installed, resulting in information sent in “clear text.”
- Because the route the email travels cannot be predicted, untrusted persons at ISP sites may read the sensitive information.
- Because the email travels over unprotected communication links, it can be “sniffed” in transit and read by an unauthorized user.
- Web browsers are often used to access private email accounts. Such access is inherently not secure, allowing others to look over the shoulder of an employee to read sensitive information or gain unauthorized access to the employee’s account.
- Many worms and viruses (which could exist on the employee’s personal computer) propagate themselves by mailing copies of existing emails or other text on a victim’s computer to unknown individuals.

- Instant Messaging and ICQ channels are a frequent source of viruses and mechanisms for attack of personal computers.
- So-called “spy ware” programs transmit information from personal computers to sites unknown to the computer’s owner. Many programs (both freeware and commercial) install these programs to harvest marketing information and other information from a user’s computer.

Any unauthorized person who acquires sensitive information in this manner could post it on the Internet, deliver it to a news bureau, or forward it to individuals who could use the information to compromise national security.

#### **5.4.8 Testing and Vulnerability Management**

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

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

A core element of vulnerability management is mitigating the discovered vulnerabilities, based on a risk management strategy. This strategy accounts for vulnerability severity, threats, and assets at risk. Risk calculation allows Components to prioritize their remediation actions, in accordance with their specific situation and risk management strategy. Remediation actions are captured in each Component’s patch management policy.

The DHS Information Security Vulnerability Management Program (ISVM), managed through the CSIRC, provides ISSMs and operational support personnel (e.g., ISSOs, System Administrators) with bulletins, alerts, and technical advisories related to emerging vulnerabilities and threats. The ISVM is modeled on the Department of Defense’s Information Assurance Vulnerability Assessment (IAVA) program but generally does not prescribe the mitigation options nor centrally manage software patching. The following ISVM tools are available to support the Component ISSM:

- DHS Top 20 Critical Vulnerabilities List
- DHS Vulnerability Assessment Team (VAT) – Red Team for Components without internal capabilities and for independent verification as necessary
- DHS Vulnerability Assessment Request Form (see Appendix O2 of DHS 4300A Attachment O to this handbook)
- Negotiated pricing for vulnerability assessment tools (pending)

The DHS Vulnerability Management Program is described in DHS 4300A Attachment O. Testing and vulnerability assessments can be accomplished by a combination of scanning and manual techniques. Plans call for DHS to field an automated C&A tool with a built-in vulnerability assessment capability. In addition, Plans of Action and Milestones (POA&Ms) will

be prepared and used in conducting periodic vulnerability testing and assessments of information security controls and techniques.

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

Testing and vulnerability assessment responsibilities are provided below.

<b>Testing and Vulnerability Assessment Responsibilities</b>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Develop and follow POA&amp;M procedures for implementing vulnerability assessments on sensitive systems.</li> <li>• Approve and manage all activities relating to requests for Vulnerability Assessment Team (VAT) assistance in support of incidents, internal and external assessments, and on-going SDLC support.</li> <li>• Ensure coordination among the DHS CSIRC, the Component CSIRC, and the Information Security Vulnerability Management (ISVM) Program when vulnerability assessments cross multiple Component responsibilities.</li> </ul> <p><b>ISSOs and IT Support Personnel</b></p> <ul style="list-style-type: none"> <li>• Support SOC/CSIRC vulnerability assessments.</li> </ul> <p><b>Other DHS personnel as required</b></p> <ul style="list-style-type: none"> <li>• TBD.</li> </ul>

## **Vulnerability Scanning**

Vulnerability scanning is the process of identifying known vulnerabilities of computing systems operating on a network for the purpose of determining if and where a system can be compromised. Vulnerability scanning often employs software that contains a database of known flaws, tests systems for the occurrence of these flaws, and generates a report of the findings that the organization can use to tighten the network's security.

Vulnerability scanning typically refers to system audits on internal networks that are not connected to the Internet, as well as systems that are visible on the Internet, in order to assess the threat of rogue software and malicious or incompetent employees in an enterprise. Its purpose is to identify weaknesses in a system (or system security procedures, hardware design, internal controls, etc.) that could be exploited to gain unauthorized access to sensitive information or affect system availability or data integrity. Internal staff members who are part of the security staff performing this type of testing should have clearance levels commensurate with that of the system. These people will intimately know the weaknesses of the Department's systems and networks.

### **Expanded Vulnerability Scanning**

The type of security testing performed by general-purpose vulnerability scanning tools may uncover weaknesses in the underlying components of systems that host DHS intranet or Internet web sites. A special class of scanning tools explores weaknesses in components of web systems for vulnerabilities related to the content and functionality of such systems. Examples of such vulnerabilities include the ability of unauthorized persons to examine or alter files, to establish cross-site scripting (which redirects users of a web site to another web site), or to directly access a database from which data is displayed on the web site.

A similar class of vulnerability tools exists for databases that have the capability of exploring inherent and design-induced weaknesses. Common vulnerabilities include default passwords that have not been removed, authentication bypass errors, and the ability to alter data without authentication.

Thorough vulnerability scanning expands upon the "canned" tools to include manual testing of potentially vulnerable systems and network components. For example, firewalls may provide barriers to standard discovery techniques. However, specialized scanning tools can utilize normally open ports (e.g., 80 for HTTP) and configurable timing parameters to discover internal systems in such a manner that neither a firewall nor a Network Intrusion Detection System (NIDS) can detect the scan. Such vulnerability assessments should also include both "war dialing" to find unauthorized dial-in modems, and "war driving" to detect unauthorized or misconfigured wireless network equipment.

### **Gap Analysis**

One type of assessment is referred to as a "gap analysis." Such testing measures the deviations in installed systems and networks from the organization's stated policies and procedures. This type of analysis requires that the testers have access to internal information such as security policy and procedure documents and specific networks or systems that should be assessed. Internal staff or, preferably, third parties can perform gap analyses.

### **Penetration Testing**

Penetration testing is a different process. Third-party personnel who have no knowledge of the security policies or the internal structure of the network typically perform penetration tests. Penetration testing assesses weaknesses of a computer facility or network to attack by amateur or professional “hackers.” A thorough penetration test will include social engineering, dumpster diving, identification of networks through public sources (e.g., WhoIs and RwhoIs searches of the Regional Internet Registries) as well as manual techniques for finding weak points in an organization’s perimeter. Once internal systems have been identified, a search of the NIST ICAT database can provide a laundry list of possible vulnerabilities in the hardware, operating systems, middleware, or applications discovered.

#### **5.4.8.1 Scope of Vulnerability Assessments**

All equipment attached to the DHS IT Infrastructure is subject to security vulnerability scanning. In today’s changing environment, vulnerable and/or unprotected systems can easily be overlooked. Systems that are not properly managed can become a potential threat to the health of the DHS infrastructure.

Proactive security scanning allows for a meaningful assessment of system security against known risks and provides a roadmap of effective countermeasures for improving security. Proactive scanning can also identify authorized and unauthorized devices on the internal network (e.g., unauthorized wireless access points, modems or high-speed [DSL] links installed by employees for their personal convenience without adequate security controls). Proactive scanning can lead to faster detection of vulnerabilities and can reduce damage to breached systems.

Reactive security scanning allows for threat quantification and assessment, accelerated damage control, and an assessment of systems against reasonable control measures during the repair/rebuilding process.

Any system identified in conjunction with a security incident will be subject to a comprehensive security scan. Random network scans will not be advertised. Network and host scans will be conducted by authorized DHS personnel using pre-designated scanning machines in order to be easily recognizable as benign activity in system log files. Because vulnerability scanning can be resource intensive, routine scanning is to be done during periods of low network activity when feasible.

#### **5.4.9 Peer-to-Peer Technology**

Peer-to-peer technology is a phrase coined to apply to individual PCs acting as servers to other individual PCs. Made popular by the music file-swapping service Napster, peer-to-peer technology allows users to share files with each other through a network of computers that use the same peer-to-peer client software. Each computer on the network has the ability to act as a both a server, by hosting files for others to download, and a client by searching other computers on the network for files the client wants to access.

Peer-to-peer technology introduces a significant risk to Government data and exposes Government agencies to legal liability for copyright infringement. Use of this technology can also decrease productivity and use large amounts of bandwidth.

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

Peer-to-peer responsibilities are provided below.

<b>Peer-to-Peer Technology Responsibilities</b>
<p><b>CIO, CISO</b></p> <ul style="list-style-type: none"> <li>Establishes DHS policy regarding the unauthorized use of IT technology and software.</li> </ul> <p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>Ensure that controls, including awareness training, are in place to minimize or prevent unauthorized use of unauthorized IT technology and software.</li> </ul> <p><b>Supervisors</b></p> <ul style="list-style-type: none"> <li>Enforce unauthorized use policies including remedial training and other sanctions.</li> <li>Promptly report unauthorized use of IT technology in accordance with DHS Computer Security Incident reporting policy (see DHS 4300A Attachment F).</li> </ul> <p><b>ISSOs, Network/System Administrators</b></p> <ul style="list-style-type: none"> <li>Ensure that controls are in place including the use of monitoring and auditing to detect unauthorized use of software</li> <li>Promptly report unauthorized use of IT technology in accordance with DHS Computer Security Incident reporting policy (see DHS 4300A Attachment F).</li> </ul> <p><b>Users</b></p> <ul style="list-style-type: none"> <li>Be aware of the prohibition against the use of unauthorized IT technology and software.</li> <li>Adhere to the unauthorized use policies established in this section and in other references provided by DHS security officials.</li> <li>Promptly report unauthorized use of IT technology in accordance with DHS Computer Security Incident reporting policy (see DHS 4300A Attachment F).</li> <li>Be aware of and understand the ramifications of penalties involving infractions of the rules regarding inappropriate use of Government resources.</li> </ul>












Peer-to-peer applications circumvent most enterprise security systems. This provides malicious users easy access to a system, allowing them to install malware on participating systems, identify IP addresses and user names of internal machines, steal classified data, launch a denial of service attack (e.g., through bandwidth consumption, filling hard disks), or gain control of network resources.

Information, including information that should be protected to respect the privacy of individuals, is also easily compromised on a machine that has peer-to-peer software installed. Many peer-to-peer programs do not allow a user to control how much of their disk space is accessible, potentially allowing files that the user has no intention of sharing to be accessed by unauthorized persons.

In addition to security concerns, the use of peer-to-peer technology for its most commonly used functions (i.e., sharing music, images, and video) exposes both the individual and DHS to criminal prosecution for copyright violations.

The use of peer-to-peer technology exposes systems to unauthorized access. Some hackers employ programs that “sniff” for open ports on a network and for an attached peer-to-peer enabled machine, automatically bypassing firewalls and other perimeter security devices. Other hackers post instructions on how to bypass firewalls through open ports.

Malware distribution is enhanced by peer-to-peer applications. Those central servers have the ability, if subverted, to distribute to all users upon connection. Other peer-to-peer systems do not use a server. Instead, when a user requests a file from a particular computer or sends a file to a particular computer, the file is passed through (and potentially deposited on) all of the intervening machines along the route between the two computers.

Most of the programs will display the IP address, MAC address, and connection speed of the computers in the peer-to-peer network. This would allow a potential intruder to identify internal components in the network that could be compromised.

For these reasons, peer-to-peer software is not authorized on DHS computers or on any computer or IT system that might be connected to the DHS network. Use of peer-to-peer software is considered an unauthorized use of Government resources and constitutes a reportable security incident and potentially can result in sanctions to the violating party.

[For additional information on inappropriate use of DHS resources, see Section 3.12, Information Technology Security Policy Violation and Disciplinary Action; Section 4.8.3, Personally Owned Equipment and Software; Section 4.8.5, Personal Use of Government Office Equipment and Department of Homeland Security Information Technology Systems/Computers; and Section 4.9, Security Incidents and Incident Response and Reporting.]

## **5.5 Cryptography**

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

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

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

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

### 5.5.1 Encryption

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

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

Encryption responsibilities are provided below.

<b>Encryption Responsibilities</b>
<p><b>CISO</b></p> <ul style="list-style-type: none"> <li>• Develops DHS cryptography policy and approves Component encryption methodologies.</li> </ul>
<p><b>DAAs</b></p> <ul style="list-style-type: none"> <li>• Ensure sensitive or classified encryption applications under their authority have developed encryption plans for IT systems prior to accreditation.</li> <li>• Ensure personnel implementing encryption requirements are technically qualified and adequately trained in encryption technologies and specific methodologies employed.</li> </ul>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Ensure DHS encryption policy is implemented and enforced.</li> <li>• Advise project managers on the implementation of DHS encryption standards.</li> </ul>
<p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure encryption methodology is properly implemented and configured on DHS systems.</li> </ul>

<b>Encryption Responsibilities</b>
<ul style="list-style-type: none"> <li>• Assist system owners in identifying sensitive DHS data that requires encryption.</li> </ul>



Encryption is a reliable and achievable way to help ensure confidentiality for sensitive data. It involves converting plain text information into an unreadable form using approved algorithms. DHS employs encryption technologies to implement requirements. These requirements include encryption of passwords, symmetric and asymmetric keys, certain activities performed by system administrators and maintenance personnel, data packets transmitted on a wireless network, and data stored on laptop devices.

Components shall ensure that encryption is addressed in the C&A documentation using DHS-approved encryption methodologies.

### 5.5.2 Public Key Infrastructure

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

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

<b>DHS Policy</b>
<p><b>a.</b> PKI policy oversight shall be provided at the Department level by a PKI Policy Authority (PKI PA). The CISO shall be the PKI PA.</p>
<p><b>b.</b> PKI operational oversight shall be provided at the Department level by a PKI Operational Authority (PKI OA) appointed by the PKI PA.</p>
<p><b>c.</b> The DHS PKI shall be governed by a DHS X.509 Certificate Policy (DHS CP). The DHS CP shall be approved by the PKI PA.</p>
<p><b>d.</b> The DHS CP must comply with the U.S. Federal PKI Certificate Policy for the Federal Bridge CA, at the high, medium, and basic assurance levels.</p>
<p><b>e.</b> DHS shall have a single High Assurance Root CA. All additional CAs within DHS must be subordinate to the DHS Root CA. The requirements and process for becoming a subordinate CA to the DHS Root CA shall be specified in the DHS CP.</p>
<p><b>f.</b> The DHS Root CA shall cross-certify with the Federal Bridge CA at the high, medium, and basic assurance levels.</p>

**DHS Policy**

**g.** Every DHS CA shall operate under an X.509 Certificate Practices Statement (CPS). The CPS for each CA must comply with the DHS CP. The DHS PKI PA must approve each CPS.

**h.** All DHS CAs shall undergo a compliance audit on a regular basis as required by CP. The DHS PKI PA shall specify a DHS PKI Auditor to review compliance audits.

**i.** All operational PKI facilities should be established in accordance with the requirements commensurate with the CA's assurance level as well as its intended use. Location/protection of the authority will be determined by its level of assurance. Measures to ensure continuity of operations of the certificate authority should be taken that are at least equal to the measures of the system being supported.

**j.** A DHS PKI archive facility shall be established to store PKI records, as required by the CP and CPSs.

**k.** Certificates that are issued by test, pilot, third party, or other CAs in DHS and that are not established as a subordinate CA to the DHS Root CA shall not be used to protect sensitive DHS data, or to authenticate to DHS operational systems containing sensitive data.

PKI responsibilities are provided below.

<b>Public Key Infrastructure Responsibilities</b>
<p><b>DAAs</b></p> <ul style="list-style-type: none"> <li>• Ensure DHS encryption policy is addressed in the security plans for IT systems that process sensitive information.</li> </ul> <p><b>CISO</b></p> <ul style="list-style-type: none"> <li>• Provides PKI oversight at the Department level.</li> <li>• Serves as the DHS PKI Policy Authority.</li> <li>• Appoints a DHS PKI Operational Authority.</li> <li>• Creates and maintains a DHS CP that complies with the U.S. Federal CP for the Federal Bridge CA.</li> <li>• Establishes and maintains the DHS PKI High Assurance Root Certificate Authority (CA).</li> <li>• Ensures that all DHS CAs are subordinate to the DHS Root CA.</li> <li>• Specifies the requirements and process for becoming a subordinate CA.</li> <li>• Authorizes subordinate CAs.</li> <li>• Ensures the DHS Root CA cross certifies with the Federal Bridge CA at the High, Medium and Basic Assurance levels.</li> <li>• Ensures that all DHS CAs operate under an approved Certification Practices Statement (CPS) that complies with the DHS CP.</li> <li>• Approves the Certification Practices Statements for all DHS CAs.</li> <li>• Ensures that all DHS CAs undergo a compliance audit at least annually, and specifies a DHS PKI Auditor to perform the compliance audits.</li> <li>• Specifies the DHS PKI Auditor to conduct the compliance audits.</li> <li>• Ensures that appropriate facilities are available for hosting DHS certificate authorities as appropriate for their level of assurance and associated mission. Ensures that appropriate continuity planning is established for all infrastructure that distributes, houses, or stores public keys.</li> <li>• Ensures that a DHS PKI archive facility is established to store PKI records.</li> <li>• Ensures that certificates issued by test, pilot, or other CAs in DHS that are not established as a subordinate CA to the DHS Root CA shall not be used to protect sensitive DHS operational data, or to authenticate to DHS operational systems containing sensitive data.</li> </ul> <p><b>PKI Operational Authority</b></p> <ul style="list-style-type: none"> <li>• Provides oversight of PKI operations at the Department level.</li> <li>• Creates and maintains all PKI CPSs pertaining to the DHS PKI.</li> <li>• Creates and manages DHS PKI Operating Procedures.</li> <li>• Oversees and reviews management of DHS PKI Operations for each authority certified subordinate to the DHS Root CA. Works with DHS and Component physical security entities and/or local registration authorities to oversee the issuance and management of certificates across the DHS enterprise.</li> <li>• Ensures that all aspects of DHS PKI services, operations and infrastructure related to certificates issued under the DHS CP are in accordance with the requirements, representations, and warranties</li> </ul>

<b>Public Key Infrastructure Responsibilities</b>
<p>of the CP.</p> <p><b>Office of Security</b></p> <ul style="list-style-type: none"> <li>Ensures that PKI registration activities under its purview are performed in compliance with the applicable CPSs.</li> </ul> <p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>Ensure that PKI registration activities under their purview are performed in compliance with the applicable CPSs.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>Ensure adequate security measures are in place to protect access to hardware and software.</li> <li>Ensure new hardware and software has been approved in accordance with the configuration management plan prior to installation.</li> </ul> <p><b>Network/System Administrators</b></p> <ul style="list-style-type: none"> <li>Ensure DHS cryptographic systems are properly configured and functioning properly.</li> </ul>










Implementation of public key infrastructure (PKI) technology, utilizing data encryption, ensures that cryptographic security goals are met. When used either separately or in conjunction with PKI, a virtual private network (VPN) greatly enhances secure data transmission, especially when encryption techniques are employed.

### 5.5.3 Public Key/Private Key

The recipient of public key certificates is referred to as a subscriber. A subscriber can be a human (e.g., an employee or contractor), an organization, an application, a code signer (e.g., digitally signs released software to enable users to authenticate its source, legitimacy, and integrity), or a device (e.g., a web server or VPN server.) Registrars are trusted PKI officials who administer the process that results in a CA issuing or revoking public key certificates for each subscriber. As part of the PKI registration process, a public key/private key pair is generated in a hardware or software cryptographic module that is under the control of the subscriber. The private key remains under the sole possession of the subscriber. A CA enters the public key into an electronic public key certificate that also identifies the owner of the key, i.e. the subscriber. The trusted CA digitally signs the certificate thereby binding the public key to the to the subscriber, and makes the signed certificate available for use by other subscribers.

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

<b>DHS Policy</b>
<p><b>a. Separate public/private key pairs must be used for encryption and digital signature by human</b></p>

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

Public key/private key responsibilities are provided below.

<b>Public Key/Private Key Responsibilities</b>
<p><b>CISO</b></p> <ul style="list-style-type: none"> <li>• Ensures that the DHS CP and CPSs enforce the use of separate public/private key pairs for encryption and digital signature by human subscribers, organization subscribers, application subscribers, code-signing subscribers, and also by device subscribers whenever supported by the protocols native to the type of device.</li> <li>• Ensures that the DHS CP and CPSs require that a human sponsor shall represent each organization, application, code-signing, and device subscriber when it applies for one or more certificates from a DHS CA.</li> <li>• Ensures that DHS CPSs require that a mechanism is provided for each DHS CA to enable PKI registrars to determine the eligibility of each proposed human, organization, application, code</li> </ul>

### **Public Key/Private Key Responsibilities**

signer, or device subscriber to receive one or more certificates.

- Ensures that DHS CPSs require that a mechanism is provided for each DHS CA to enable PKI registrars to determine the authorized human sponsor for each organization, application, code signer, or device.
- Ensures that controls are implemented to hold human subscribers accountable for the security of their private key and for all transactions signed with their private key.
- Ensures that controls are implemented to hold the sponsor of an organization, application, code signing, or device subscriber responsible for the security of and use of the subscriber's private keys.
- Ensures that controls are implemented to maintain individual accountability for each use of a shared organizational or code signing private key.
- Ensures that a DHS PKI Subscriber Agreement for Human Users and a DHS PKI Subscriber Agreement for Sponsors are created and maintained, and that DHS CPSs require human subscribers and sponsors to read, understand and sign them as a pre-condition for receiving certificates.

#### **PKI Operational Authority**

- Ensures that the DHS CPSs and operating procedures enforce the use of separate public/private key pairs for encryption and digital signature by human subscribers, organization subscribers, application subscribers, code-signing subscribers, and also by device subscribers whenever supported by the protocols native to the type of device.
- Ensures that the DHS CPSs and operating procedures require that a human sponsor shall represent each organization, application, code-signing, and device subscriber when it applies for one or more certificates from a DHS CA.
- Verifies that that a mechanism is provided for each DHS CA to enable PKI registrars to determine the eligibility of each proposed human, organization, application, code signer, or device subscriber to receive one or more certificates.
- Verifies that a mechanism is provided for each DHS CA to enable PKI registrars to determine the authorized human sponsor for each organization, application, code signer, or device.
- Verifies that controls are implemented to hold human subscribers accountable for the security of their private key and for all transactions signed with their private key.
- Verifies that controls are implemented to hold the sponsor of an organization, application, code signing, or device subscriber responsible for the security of and use of the subscriber's private keys.
- Verifies that controls are implemented to maintain individual accountability for each use of a shared organizational or code signing private key.
- Ensures that DHS CPSs and Operating Procedures require human subscribers and sponsors to read, understand, and sign DHS PKI Subscriber Agreements as a pre-condition for receiving certificates.

#### **Office of Security**

- Provides a mechanism, as required by the CPS, to enable PKI registrars to determine the eligibility of each proposed human subscriber to receive one or more certificates from the DHS CA.
- Ensures that registrars under their purview require human subscribers and sponsors to read, understand and sign DHS PKI Subscriber Agreements as a pre-condition for receiving certificates.

#### **ISSMs**

- Provide a mechanism, as required by the CPS, to enable PKI registrars to determine the eligibility of each proposed human subscriber to receive one or more certificates from the DHS CA.

### **Public Key/Private Key Responsibilities**

- Provide a mechanism, as required by the CPS, to enable PKI registrars to determine the authorized human sponsor for each organization, application, code signer, or device.
- Implement controls to hold human subscribers accountable for the security of their private key and for all transactions signed with their private key.
- Implement controls to hold the sponsor of an organization, application, code signing, or device subscriber responsible for the security of and use of the subscriber's private keys.
- Implement controls to maintain individual accountability for each use of a shared organizational or code signing private key.
- Ensure that registrars under their purview require human subscribers and sponsors to read, understand and sign DHS PKI Subscriber Agreements as a pre-condition for receiving certificates.

#### **ISSOs**

- Ensure human subscribers are aware of their responsibilities to protect their private keys.
- Ensure sponsors are aware of their responsibilities to protect the private keys of the subscriber they sponsor.
- Maintain auditable records to ensure individual accountability is maintained for each use of an organization or code-signing private key authorized for use by more than one person.

#### **Human Subscribers**

- Assume responsibility for the security of their private keys.
- Abide by the DHS PKI Subscriber Agreement for Human Users that they signed, and review it at least annually.

#### **Sponsors**

- Assume responsibility for the security of the private keys of the subscribers they sponsor.
- Abide by the DHS PKI Subscriber Agreement for Sponsors that they signed, and review it at least annually.

DHS employees should have reasonable assurance that, when initiating a secure transaction:

- The information sender and recipient both will be identified uniquely so that both parties know not only where the information originated but also its destination
- The information was not altered deliberately or inadvertently
- The sender's identity is inextricably linked to the transmitted information
- The information will be protected from unauthorized use.

## **5.6 Virus Protection**

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

There are a number of programs that are classified as malicious code. These programs are called such things as viruses, logic bombs, worms, and Trojan horses. This section covers viruses and other types of malicious code.

<b>DHS Policy</b>
<b>a.</b> ISSMs shall establish and enforce Component-level virus protection control policies.
<b>b.</b> Components shall implement a defense-in-depth strategy that: <ul style="list-style-type: none"> <li>– Installs antivirus software on desktops and servers</li> <li>– Configures antivirus software on desktops and servers to check all files, downloads, and email</li> <li>– Installs updates to antivirus software and signature files on desktops and servers in a timely and expeditious manner without requiring the end user to specifically request the update</li> <li>– Installs security patches to desktops and servers in a timely and expeditious manner.</li> </ul>
<b>c.</b> Components may implement appropriate file/protocol/content filtering to protect their data and networks in accordance with their Internet usage policy.



Virus protection responsibilities are provided below.

<b>Virus Protection Responsibilities</b>
<p><b>ISSMs</b></p> <ul style="list-style-type: none"> <li>• Establish and enforce virus protection control policy.</li> <li>• Provide technical expertise and evaluate the effectiveness of virus protection approaches.</li> </ul> <p><b>Certifying Officials</b></p> <ul style="list-style-type: none"> <li>• Ensure that vulnerability to viruses and other malicious code is detailed in the risk analysis section of the C&amp;A documentation and that adequate steps to mitigate that risk are taken for each system.</li> </ul> <p><b>System Owners</b></p> <ul style="list-style-type: none"> <li>• Assess the impacts associated with system downtime caused by viruses and other malicious code and ensure adequate resources are allocated to address continuity of operations.</li> </ul> <p><b>System/Network Administrators</b></p> <ul style="list-style-type: none"> <li>• Ensure that all DHS IT systems employ virus protection software.</li> <li>• Ensure that antivirus software is installed on every workstation, network, laptop, and mobile computing device.</li> <li>• Update virus signature files immediately with each new release.</li> <li>• Ensure that virus protection software employs resident scanning.</li> <li>• Ensure that virus scanning occurs automatically during boot-up and installation of new software.</li> <li>• Ensure that all diskettes are scanned for viruses prior to use (including blank disks).</li> <li>• Follow procedures detailed in this manual in the event that a virus is detected.</li> </ul> <p><b>ISSOs</b></p> <ul style="list-style-type: none"> <li>• Employ virus prevention measures commensurate with the level of risk identified for virus infections in the risk analysis.</li> <li>• Ensure that procedures are implemented to prevent, detect, eradicate, and report computer virus incidents.</li> <li>• Ensure that virus incidents are reported in accordance with CSIRC procedures (see Section 4.9).</li> </ul>

### Virus Protection Responsibilities

#### Users

- Ensure that no files are downloaded or opened from unknown or untrusted sources. All files should be scanned by antivirus software before opening them. Do not open suspicious email.
- Notify the System / Network Administrator if antivirus software is not installed on the user workstation.
- Never disable antivirus software functions.
- Report virus and other malicious code incidents in accordance with procedures described in Section 4.9, Security Incidents and Incident Response and Reporting.

#### 5.6.1 What Is a Virus?

A virus is a self-replicating malicious program segment that attaches itself to legitimate applications programs, operating system commands, or other executable system components and spreads from one system to another. It can also be defined as a program or piece of code that is loaded onto a computer without the user's knowledge and runs against the user's wishes. As it spreads, it is said to be *infecting* the system.

- A computer virus may only be a line or two of programming code hidden within a program.
- It can be benign and limited to sending a greeting to amuse or annoy, or malicious, written specifically to damage other programs.
- It can display a message, erase files, subtly alter stored data, or "crash" a hard drive.

#### 5.6.2 Other Types of Malicious Code

Other types of malicious code can be defined according to the following table:

Table 7: Types of Malicious Code

**Worms:** Computer worms are malicious programs that copy themselves from system to system, rather than infiltrating legitimate files. For example, a mass-mailing email worm is a worm that sends copies of itself via email. A network worm makes copies of itself throughout a network or through file shares. Worms often contain Trojan horse or "backdoor" programs.

**Logic Bombs:** A logic bomb can be defined as dormant code, the activation of which is triggered by a predetermined time or event. For example, a logic bomb might start erasing data files when the system clock reaches a certain date or when the application has been loaded X number of times.

**Trojan Horses:** A Trojan horse is a computer program that is apparently or actually useful but performs another function. A Trojan horse generally provides remote control access to an unauthorized person. A Trojan horse can be used to modify databases, write checks, send email, or destroy files. It could be imbedded by a programmer or downloaded from the Internet.

**Web Bugs:** A web bug is executable code included in an image (as small as one pixel) that can disrupt the operation of a system or acquire and transmit information from a system without the user's knowledge by merely visiting a malicious or compromised web site.

### 5.6.3 How Viruses and Other Malicious Code Affect Systems

Regardless of the type of malicious code, viruses and other malicious code can pose a significant threat to DHS systems, which can affect the availability, integrity and confidentiality of information and processing resources. *Therefore, it is essential that all systems employ prevention measures commensurate with the level of risk identified in the risk analysis.* What makes viruses and other malicious code different from other problems is that they can spread—from program to program and from system to system—*without direct human intervention.*

Systems that can be accessed by DHS-approved browser configurations should be categorized (trusted, untrusted, etc.). Users are not allowed to deploy Web browsers “out of the box,” since the security policies implemented in such tools tend to reflect the vendor’s interests and do not necessarily coincide with those of DHS.

### 5.6.4 Procedures When a Virus Is Detected on a System

If a virus or other malicious code is detected, the LAN/system administrator is responsible for taking appropriate actions to eradicate the problem. Such actions include:

- Running disinfectors available with antivirus software
- Scanning backup diskettes and tapes for viruses prior to restoring system applications and data files
- Checking for re-infection from overlooked disks or other media during the eradication process
- Notifying the ISSO of the security incident via incident reporting procedures described in Section 4.9.

Once the malicious code has been eradicated, the system administrator shall determine the extent of the damage and restore all damaged files or programs to uninfected files and programs. Backup media should be scanned *prior to restoring* system applications and data files.

Note that occurrences of malicious code constitute a *security incident* that must be reported; reporting procedures are described in Section 4.9, Security Incidents and Incident Response and Reporting.

## 5.7 Product Assurance

Information assurance (IA) involves protecting and defending information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. Information assurance is achieved through the use of IA and IA-enabled products.

DHS Policy
<p><b>a.</b> Information Assurance (IA) shall be considered a requirement for all systems used to enter, process, store, display, or transmit sensitive or national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated commercial off-the-shelf (COTS) IA and IA-enabled IT products. These products shall provide for the availability of systems. The products also shall ensure the integrity and confidentiality of information and the authentication and</p>

<b>DHS Policy</b>
nonrepudiation of parties in electronic transactions.
<p><b>b.</b> <i>Strong preference</i> shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting sensitive information) that have been evaluated and validated, as appropriate, in accordance with the following:</p> <ul style="list-style-type: none"> <li>– The NIST FIPS validation program.</li> <li>– The National Security Agency (NSA)/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program</li> <li>– The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement</li> </ul>
<p><b>c.</b> The evaluation and validation of COTS IA and IA-enabled IT products shall be conducted by accredited commercial laboratories or by NIST.</p>
<p><b>d.</b> Components shall use only cryptographic modules that have been validated in accordance with FIPS 140-2.</p>

Product assurance responsibilities are provided below.

<b>Product Assurance Responsibilities</b>
<p><b>CISO/ISSMs</b></p> <ul style="list-style-type: none"> <li>• Provide guidance in the use of COTS information assurance products.</li> </ul>
<p><b>Certifying Officials</b></p> <ul style="list-style-type: none"> <li>• Validate the proper use of information assurance products.</li> </ul>
<p><b>System Administrators/ISSOs</b></p> <ul style="list-style-type: none"> <li>• Ensure selected information assurance products are properly deployed and configured.</li> </ul>
<p><b>IT Project Managers</b></p> <ul style="list-style-type: none"> <li>• Comply with product assurance policy during system development.</li> </ul>

The National Information Assurance Partnership (NIAP), a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA), is a U.S. Government initiative designed to meet the security testing, evaluation, and assessment needs of both IT producers and consumers. NIAP combines the extensive security experience of both agencies to promote the development of technically sound security requirements for IT products and systems and appropriate metrics for evaluating those products and systems.

The NIAP Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS) is a partnership between the public and private sectors, to evaluate IT product conformance to international standards. This program is being implemented to help consumers select commercial off-the-shelf IT products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace.

DHS Components are to keep apprised of the above ongoing initiatives and to strongly consider the recommendations and findings of the NIAP in the selection of COTS products. This guidance applies to both stand-alone COTS products as well as those incorporated in other IT systems. Compliance with this policy, coupled with the restriction that the products have been appropriately validated by the designated Federal authorities and the Common Criteria, will reduce costs and remove the burden of maintaining and providing interoperability between numerous custom written software systems by a variety of contractors.

## **6.0 DOCUMENT CHANGE REQUESTS**

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

## **7.0 QUESTIONS AND COMMENTS**

For clarification of DHS IT security policies or procedures, contact the DHS Director for IT Security Policy at [INFOSEC@dhs.gov](mailto:INFOSEC@dhs.gov).