

# **INFORMATION SECURITY**

## **POLICY (ISP)**

**FOR**

**THE SOCIAL SECURITY ADMINISTRATION (SSA)**



**OFFICE OF INFORMATION SECURITY**

**SEPTEMBER 26, 2019**

**VERSION 2.7**

## INFORMATION SECURITY POLICY (ISP)

### REVISION HISTORY

Use the table in this section to track revisions to the chapter. They will be added to the document Revision History page located in the beginning of the document after the Table of Contents. Leave blank any column for which you are unsure of content (i.e., if you are not the Reviewer / Approver, you would leave the last 3 columns blank).

Version	Revision Date	Brief Description	Author(s)	Last Reviewed Date	Reviewed / Approved by	Effective Date
1.0	01/11/2019	Initial publication of the Cybersecurity Framework-aligned ISP.	(b) (7)(E)	NA	(b) (7)(E)	01/11/2019
1.1	01/18/2019	Added Section 3.1.9, Mobile Device Security, using the same text from ISP version 10.5 (11/16/2018) Removal of SAM Grade requirement – Appendix 7.2 Addition of CISO responsibility as Cybersecurity Risk Executive – Appendix 7.2	(b) (7)(E)	NA	(b) (7)(E)	01/18/2019
1.2	01/28/2019	Re-inserted missing Remediation Section into Section 2.1.1.3	(b) (7)(E)	NA	(b) (7)(E)	01/28/2019

## INFORMATION SECURITY POLICY (ISP)

		<p>Re-inserted missing Configuration Requirements for (b) (7)(E) Section into Section 3.4.1.1.</p> <p>Re-inserted missing Exceptions Section into Section 3.4.1.2.</p>				
1.3	02/04/2019	<p>Updated CIO and CISO Roles and Responsibilities in Section 7.2 to reference (b) (7)(E) Delegation of Authority as Cybersecurity Risk Executive.</p>	(b) (6)	02/04/2019	(b) (6)	02/04/2019
1.4	02/06/2019	<p>Re-inserted missing sub-sections into Wireless Technology policy in Section 3.1.6.</p> <p>Re-inserted missing sub-sections into Audit Trail Requirements policy in Section 3.6.1.1.</p> <p>Updated link to Audit (b) (7)(E) in Section 3.6.1.1.3.</p>	(b) (7)(E) (b) (6)	02/06/2019	(b) (6) (b) (6)	02/06/2019
1.5	02/07/2019	<p>Updated Access Management section in Section 3.1.3.1 to clarify review requirements for security reports.</p>	(b) (6) (b) (6)	02/07/2019	(b) (6)	02/07/2019

1.6	02/13/2019	<p>Updated the name of the Records Management site in Section 3.3.10.</p> <p>Clarified System Security Plan (SSP) requirements and responsibilities in Sections 2.4.1.2 and 7.2.</p>	<p>(b) (6)</p> <p>(b) (6)</p> <p>(b) (6)</p>	02/13/2019	(b) (6)	02/13/2019
1.7	03/07/2019	<p>Updated link to CUI Policy in the Rules of Behavior in Section 1.2.2.5.</p> <p>Revised previous reference to DSCS security configuration guides in Section 3.1.4.4.</p> <p>Updated (b) (7)(E) link in Section 3.6.1.</p> <p>Updated links to referenced ISP sections in Section 3.6.2.5.5.</p>	(b) (6)	03/07/2019	<p>(b) (6)</p> <p>(b) (6)</p>	03/07/2019
1.8	03/11/2019	<p>Updated link to referenced Reporting section in Section 1.2.2.9.</p> <p>Updated link to referenced Audit Trail System section in Section 3.1.3.2.</p> <p>Updated link to referenced Multi-homing section in Section 3.1.4.4.</p>	(b) (6)	03/11/2019	(b) (6)	03/11/2019

		<p>Updated link to referenced Audit Trail System section in Section 3.1.7.1.</p> <p>Updated link to referenced Role-based Training section in Section 3.6.1.1.2.</p> <p>Updated link to referenced Reporting section in Section 7.2 - Appendix B.</p>				
1.9	04/01/2019	<p>Revised CIO Roles and Responsibilities in Section 7.2 – Appendix B to reflect responsibilities in the event that there is a change in the CIO.</p> <p>Updated link to SSA Memorandum 2019-003 Delegation of Authority as Cybersecurity Risk Executive in CISO Roles and Responsibilities in Section 7.2 – Appendix B.</p>	(b) (6)	03/29/2019	(b) (6)	04/01/2019
2.0	05/08/2019	<p>Updated (b) (7)(E), (b) (2) [REDACTED] in Section 3.4.7.</p> <p>Updated link to ATS SharePoint site in Section 3.6.1.</p>	(b) (6)	05/08/2019	(b) (6)	05/08/2019
2.1	05/17/2019	<p>Updated link to ISO Manual in Sections 2.1.4, 3.1.1, 3.1.1.1, 3.1.1.2, 3.1.3.1, and 7.2 – Appendix B.</p>	(b) (6)	05/17/2019	(b) (6)	05/17/2019

		<p>Updated link to Account Type Matrix in Sections 3.1.1.2 and 3.1.3.</p> <p>Updates link to Encrypting Files Using (b) (7)(E) document in Section 3.3.5.</p> <p>Updated Non-Disclosure Agreement for Removal of SSA Sensitive Information document in Section 7.2 – Appendix B.</p>				
2.2	05/22/2019	<p>Updated links to various documents throughout ISP.</p>	(b) (6)	05/22/2019	(b) (6)	05/22/2019
2.3	06/18/2019	<p>Revised Asset Management Policy in Section 2.1 to better define Information System boundaries and SSA's (b) (7)(E) [redacted]. Included a link to the Cyber Risk Management Strategy document.</p> <p>Revised Web Services Security Policy in Sections 3.1.7, 3.3.1.3 and 3.6.4 to better align with current authentication and authorization trends.</p> <p>Revised Web Application Development Rules in Section 3.4.3 to stipulate that all application code must be stored in an Agency-approved platform.</p>	<p>(b) (6)</p> <p>(b) (6)</p> <p>(b) (6)</p> <p>(b) (6)</p>	06/14/2019	<p>(b) (6)</p> <p>(b) (6)</p>	06/18/2019

		<p>Updated links throughout Web Application Development Policy in Section 3.4.3.</p> <p>Updated email address for inquiries relating to FTI in Section 4.1.3.3.</p> <p>Removed references to outdated Non-Disclosure Agreement (NDA) in Section 7.2.</p>				
2.4	08/01/2019	<p>Revised the Configuration Management Policy in Section 3.4.1 to require updated patching for operating systems and application software.</p>	(b) (6)	08/02/2019	(b) (6)	08/02/2019
2.5	08/22/2019	<p>Revised the Media Sanitization Policy in Section 3.4.6 to include a link to the updated Personal Property Management Handbook.</p> <p>Corrected the references to ISP Section 2.1.2 in Sections 1.2.2.6 and 3.1.9.1.</p>	(b) (6)	08/22/2019	(b) (6)	08/22/2019
2.6	09/18/2019	<p>Added link to SSA's Social Media Management Policy in Section 1.2.2.8.</p> <p>Updated link to NIST 800-16 reference in Section 3.2.1.</p> <p>Included link to Encryption Methods page in Section 3.3.5.</p>	(b) (6)	09/18/2019	(b) (6)	09/18/2019

2.7	09/26/2019	Modified the Credential Management policy in Section 3.1.1.2 to specify the password requirements for Service Accounts. The Credential Rules and Requirements page was also updated to reflect password rules and requirements for Service Accounts.	(b) (6)	09/26/2019	(b) (6)	09/26/2019
-----	------------	--	---------	------------	---------	------------

SSA CONFIDENTIAL INFORMATION



# INFORMATION SECURITY POLICY (ISP)

## TABLE OF CONTENTS

<b>1</b>	<b>Section I: Overview of Information Security .....</b>	<b>1</b>
1.1	Introduction .....	1
1.2	Rules of Behavior for Users and Managers of Information Resources.....	2
1.2.1	Management Responsibilities.....	2
1.2.2	User Responsibilities.....	2
1.2.2.1	Accountability.....	2
1.2.2.2	Integrity .....	3
1.2.2.3	Confidentiality.....	3
1.2.2.4	Awareness and Training.....	3
1.2.2.5	Sensitive Information .....	3
1.2.2.6	Hardware, Software, and Copyright Protection and Control .....	3
1.2.2.7	Alternative Worksite (Non-SSA Controlled Locations).....	4
1.2.2.8	Public Disclosure .....	4
1.2.2.9	Incident Reporting.....	5
1.2.3	Consequences of Rules Violations .....	5
<b>2</b>	<b>Section II: Identify .....</b>	<b>1</b>
2.1	Asset Management.....	1
2.1.1	Platform Boundary.....	1
2.1.2	Authorized Hardware and Software.....	1
2.1.2.1	Remediation .....	2
2.1.3	Information System Boundary.....	2
2.1.4	IT Systems and Inventory.....	2
2.1.5	Information System Interconnections and Information Flow .....	3
2.1.6	Security Categorization and Prioritization .....	3
2.1.7	CyberSecurity Roles and Responsibilities .....	5
2.2	Business Environment .....	6

## INFORMATION SECURITY POLICY (ISP)

2.2.1	Supply Chain Risk Management.....	6
2.2.2	Contingency Planning .....	6
2.2.2.1	Information System Contingency Planning.....	7
2.2.2.2	Contingency Planning Policy .....	8
2.3	Governance .....	9
2.3.1	Information Security Policy.....	9
2.3.2	Security Organization Structure .....	10
2.3.3	Laws and Regulations .....	11
2.4	Risk Assessment .....	12
2.4.1	Security Assessment and Authorization (SA&A).....	12
2.4.1.1	The SSA Risk Management Framework (RMF) Process.....	12
2.4.1.2	System Security Plan (SSP) .....	13
2.4.2	Threat and Vulnerability Management.....	13
2.4.3	Information System Risk Assessment.....	13
2.4.4	Additional Information.....	15
2.5	Risk Management Strategy .....	15
2.5.1	Risk Management.....	15
3	Section III: Protect.....	1
3.1	Access Control.....	1
3.1.1	Identity and Credential Management.....	1
3.1.1.1	Identity Management.....	2
3.1.1.2	Credential Management.....	2
3.1.1.3	Password Policy .....	4
3.1.2	Remote Access .....	5
3.1.3	Account Policy .....	5
3.1.3.1	Access Management.....	6
3.1.3.2	Systems Access Security Administration .....	8
3.1.3.3	Sanctions for Unauthorized Systems Access .....	8
3.1.4	Network Integrity and Protection .....	9
3.1.4.1	Network Segmentation.....	9

## **INFORMATION SECURITY POLICY (ISP)**

3.1.4.2	Multi-Homing.....	9
3.1.4.3	Modems in SSA Facilities .....	9
3.1.4.4	Broadband Internet Connections in SSA Facilities .....	9
3.1.4.5	Restricted Hardware and Software.....	10
3.1.4.6	Prohibited Security Practices / Activities .....	10
3.1.5	<b>Limited Personal Use of Government Office Equipment, Including IT</b> .....	<b>11</b>
3.1.6	<b>Wireless Technology</b> .....	<b>11</b>
3.1.6.1	Mobile Computing Devices.....	11
3.1.6.2	Personally Owned Mobile Computing Devices .....	11
3.1.6.3	Prohibited Wireless Technology.....	12
3.1.6.4	Wireless Exception.....	12
3.1.7	<b>Web Services Security</b> .....	<b>12</b>
3.1.7.1	Background.....	12
3.1.7.2	External Clients (Accessing SSA Web Services from outside of SSANet).....	13
3.1.8	<b>Cloud Security</b> .....	<b>14</b>
3.1.8.1	Background.....	14
3.1.8.2	Procedure .....	14
3.1.8.3	Cloud Deployment Model .....	15
3.1.8.4	FedRAMP Security Requirements .....	15
3.1.8.5	Agency Security Requirements .....	16
3.1.8.6	Chief Information Officer Approval.....	16
3.1.9	<b>Mobile Device Security</b> .....	<b>17</b>
3.1.9.1	Background.....	17
3.1.9.2	International Travel .....	17
3.2	<b>Awareness and Training</b> .....	<b>19</b>
3.2.1	Information Security Training and Awareness Policy.....	19
3.2.2	Role-Based Training for Personnel with Significant Cybersecurity Responsibilities.....	19
3.2.3	Training Records Retention .....	20
3.2.4	Agency Reporting of Information Security Training .....	20
3.3	<b>Data Security</b> .....	<b>20</b>
3.3.1	Protection of Information in Transit and at Rest .....	20

## **INFORMATION SECURITY POLICY (ISP)**

3.3.1.1	Laptop Encryption .....	21
3.3.1.2	Removable Media Encryption .....	21
3.3.1.3	Key Management .....	22
<b>3.3.2</b>	<b>Data Protection throughout the Lifecycle .....</b>	<b>22</b>
3.3.2.1	Data Custodianship .....	22
3.3.2.2	Removable Media .....	23
3.3.2.3	Handling and Exchange .....	23
3.3.2.4	Definitions .....	23
<b>3.3.3</b>	<b>Data Integrity .....</b>	<b>25</b>
3.3.3.1	Automated Integrity Reviews .....	25
<b>3.3.4</b>	<b>IT Equipment Safeguards .....</b>	<b>25</b>
<b>3.3.5</b>	<b>Secure Email Use Policy.....</b>	<b>25</b>
<b>3.3.6</b>	<b>Secure Fax Use Policy .....</b>	<b>28</b>
<b>3.3.7</b>	<b>Prohibited Security Practices / Activities.....</b>	<b>29</b>
<b>3.3.8</b>	<b>IRS Federal Tax Information (FTI).....</b>	<b>29</b>
3.3.8.1	Directive .....	29
3.3.8.2	What is FTI? .....	29
<b>3.3.9</b>	<b>Disclosure Policy .....</b>	<b>30</b>
<b>3.3.10</b>	<b>Records Retention Policy.....</b>	<b>30</b>
<b>3.3.11</b>	<b>Mandatory Encryption of Electronic Data on Mobile Computers and Devices .....</b>	<b>30</b>
<b>3.3.12</b>	<b>Other Agency Guidance on Email/Fax Not Listed Above .....</b>	<b>30</b>
<b>3.3.13</b>	<b>Paper Records Disposal .....</b>	<b>30</b>
<b>3.4</b>	<b>Information Protection Process Policy .....</b>	<b>31</b>
<b>3.4.1</b>	<b>Configuration Management.....</b>	<b>31</b>
3.4.1.1	Security Configuration Standards .....	32
3.4.1.2	Exceptions .....	32
<b>3.4.2</b>	<b>System Development Lifecycle Security.....</b>	<b>32</b>
3.4.2.1	Information Technology (IT) Contract Requirements .....	33
<b>3.4.3</b>	<b>Web Application Development Policy .....</b>	<b>34</b>
3.4.3.1	Web Application Development Rules .....	34
<b>3.4.4</b>	<b>Configuration Change Control.....</b>	<b>35</b>
<b>3.4.5</b>	<b>System Backup .....</b>	<b>35</b>

## INFORMATION SECURITY POLICY (ISP)

<b>3.4.6</b>	<b>Media Sanitization</b> .....	<b>36</b>
<b>3.4.7</b>	<b>Continuous Monitoring</b> .....	<b>37</b>
<b>3.4.8</b>	<b>Incident Response</b> .....	<b>38</b>
<b>3.4.9</b>	<b>Personnel Screening</b> .....	<b>39</b>
<b>3.5</b>	<b>Maintenance</b> .....	<b>41</b>
<b>3.5.1</b>	<b>Controlled Maintenance</b> .....	<b>41</b>
<b>3.5.2</b>	<b>Remote Maintenance</b> .....	<b>41</b>
<b>3.6</b>	<b>Protective Technology</b> .....	<b>41</b>
<b>3.6.1</b>	<b>Audit Trail Systems</b> .....	<b>41</b>
<b>3.6.1.1</b>	<b>Audit Trail Requirements</b> .....	<b>42</b>
3.6.1.1.1	Use of Audit Data .....	43
3.6.1.1.2	Distribution of Audit Data .....	44
3.6.1.1.3	Audit (b) (7)(E) Core Services .....	44
3.6.1.1.4	Additional Audit Coverage Areas .....	44
3.6.1.1.5	System-Level.....	44
3.6.1.1.6	Application Level .....	44
3.6.1.1.7	Individuals of Extraordinary National Prominence (IENP) and Own SSN Requirements.....	44
<b>3.6.2</b>	<b>System Logging Requirements</b> .....	<b>45</b>
<b>3.6.2.1</b>	<b>Logged Events</b> .....	<b>45</b>
<b>3.6.2.2</b>	<b>Event Log Elements</b> .....	<b>46</b>
<b>3.6.2.3</b>	<b>Log Review and Update</b> .....	<b>46</b>
<b>3.6.2.4</b>	<b>Event Log Access</b> .....	<b>46</b>
<b>3.6.2.5</b>	<b>Log Format and Storage</b> .....	<b>46</b>
3.6.2.5.1	File Integrity Check Required .....	47
3.6.2.5.2	Retention.....	47
3.6.2.5.3	Categorization .....	47

## INFORMATION SECURITY POLICY (ISP)

3.6.2.5.4	Requirements .....	47
3.6.2.5.5	Definitions .....	48
<b>3.6.3</b>	<b>Removable Media and Protection from Data Loss Policy .....</b>	<b>49</b>
3.6.3.1	Removable Media Devices.....	49
3.6.3.2	Data Loss Protection.....	49
3.6.3.3	Local Manager Responsibilities.....	50
<b>3.6.4</b>	<b>Access Enforcement.....</b>	<b>50</b>
<b>3.6.5</b>	<b>Communication and Control Network Protection .....</b>	<b>50</b>
3.6.5.1	Network Boundary Protection.....	50
3.6.5.2	Network Control Devices .....	51
3.6.5.3	Peer-to-Peer (P2P) and Web Conferencing / Collaboration Technologies .....	52
3.6.5.4	Instant Messaging .....	52
<b>4</b>	<b>Section IV: Detect.....</b>	<b>1</b>
<b>4.1</b>	<b>Anomalies and Events .....</b>	<b>1</b>
<b>4.1.1</b>	<b>Network and Security Operations.....</b>	<b>1</b>
<b>4.1.2</b>	<b>Security Event Analysis and Response .....</b>	<b>2</b>
<b>4.1.3</b>	<b>Reporting .....</b>	<b>2</b>
4.1.3.1	Incidents Relating to Program and Employee Fraud.....	3
4.1.3.2	Reporting Loss of Personally Identifiable Information (PII).....	3
4.1.3.3	Reporting Unauthorized Federal Tax Information (FTI) Access or Improper FTI Disclosure .....	3
4.1.3.4	Criminal Violations and Fraud Policy .....	4
4.1.3.4.1	Violations Reporting Process.....	4
4.1.3.4.2	Programmatic Violations.....	4
4.1.3.4.3	Employee Violations.....	5
4.1.3.4.4	SSA Fraud Hotline.....	5
4.1.3.4.5	Request for Assistance by SSA OIG.....	5
4.1.3.4.6	Request for Information by Other Law Enforcement Agencies and Investigators.....	5

## INFORMATION SECURITY POLICY (ISP)

<b>4.2</b>	<b>Security Continuous Monitoring</b> .....	<b>5</b>
<b>4.2.1</b>	<b>Personnel Activity Monitoring</b> .....	<b>5</b>
4.2.1.1	Email and Fax Monitoring.....	5
<b>4.2.2</b>	<b>Malicious Code Detection</b> .....	<b>6</b>
<b>4.2.3</b>	<b>Service Provider Monitoring</b> .....	<b>6</b>
<b>4.2.4</b>	<b>Monitoring for Unauthorized Connections, Devices, and Software</b> .....	<b>6</b>
<b>4.2.5</b>	<b>Vulnerability Scanning</b> .....	<b>6</b>
<b>5</b>	<b>Section V: Respond</b> .....	<b>1</b>
<b>5.1</b>	<b>Response Planning</b> .....	<b>1</b>
<b>5.2</b>	<b>Communications</b> .....	<b>1</b>
<b>5.3</b>	<b>Analysis</b> .....	<b>2</b>
5.3.1	Security Event Notification.....	2
5.3.2	Impact Analysis.....	2
<b>5.4</b>	<b>Mitigation</b> .....	<b>2</b>
5.4.1	Incident Handling .....	2
5.4.2	Information Sharing and Reporting.....	2
<b>6</b>	<b>Section VI: Recover</b> .....	<b>1</b>
<b>6.1</b>	<b>Recovery Planning</b> .....	<b>1</b>
<b>6.2</b>	<b>Improvements</b> .....	<b>1</b>
<b>7</b>	<b>Section VII: Appendices</b> .....	<b>1</b>
	<b>Appendix A: Requests for Waivers from Information Security Policy (ISP)</b>	
	<b>Policies</b> .....	<b>1</b>
	<b>Appendix B: Roles and Responsibilities</b> .....	<b>2</b>

# 1 Section I: Overview of Information Security

## 1.1 Introduction

**Introduction:** The Social Security Administration (SSA), Office of Information Security (OIS) developed the Information Security Policy (ISP) to serve as protocol to protect the agency's Information Technology (IT) resources and data, to manage risk in a secure environment. The Federal Information Security Modernization Act (FISMA) of 2014 (44 USCA 3534) requires the SSA Chief Information Officer (CIO), through the Commissioner, to establish an agency-wide Information Security program, and the supporting policies to support that program. The security program and its policies implement Information Security controls based on the risk and level of harm which results from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected, or maintained, by or on behalf of the agency. FISMA also requires that all senior agency officials provide Information Security for the information and Information Systems that support the operations and assets under their control.

Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," established the development of a Cybersecurity Framework (CSF), a voluntary risk-based set of standards and practices for organizations to manage cybersecurity risk using five core functions: Identify, Protect, Detect, Respond and Recover. "The Framework for Improving Critical Infrastructure Cybersecurity", published by the National Institute of Standards and Technology is the result of a collaboration between the public and private sectors and maps NIST Special Publication (SP) 800-53 Revision 4 controls to CSF categories. The ISP has been developed to align with the CSF.

**Purpose:** The ISP sets forth Information Security standards for the protection of Non-Public Information at SSA. Maintaining the confidentiality, integrity, availability, and regulatory compliance of Non-Public Information stored, processed, and / or transmitted at SSA is a requirement of all Authorized Users. This policy applies to information in any format, including electronic and hard copy. Users are required to report any violations of this policy to the individual's manager or the appropriate SSA official. Violations may result in disciplinary action in accordance with applicable SSA policies.

**Scope:** This policy applies to all personnel acting on behalf of the agency and for personnel using agency Information Systems. This policy applies to all SSA employees, including Disability Determination Services (DDS) employees, temporary staff, contractors, and other users who act on behalf of SSA or access SSA Information Systems resources, hereafter referred to as "SSA Employee(s)". It is important to note that, due to the unique relationship with the DDSs, supplemental regulations / guidance and specific agency policy are coordinated and distributed through SSA's Office of Disability Determinations (ODD) in the Office of Operations.

Definitions for the terms used in the document provided in [ISP Definitions](#). The references used in this document are compiled and listed in Information Security Policy Appendix: [References](#). These documents are maintained in the security ecosystem.



## 1.2 Rules of Behavior for Users and Managers of Information Resources

The rules of behavior are required of all Executive Branch government agencies, and departments by [OMB Circular A-130, Appendix III](#) and these rules governed on Federal laws, regulations, and SSA directives. Failure to follow these prescribed rules, and / or misuse of information resources, can lead to suspension, termination, or other administrative or legal actions based on the seriousness of the violation.

The rules of behavior convey information about SSA security requirements, expectations, roles, and responsibilities to SSA Information Systems and resources users, and applies to all employees, contractors, DDS employees, volunteers, and anyone granted access to SSA Information Systems and / or data. These rules apply to users at their primary workplace and at any alternative workplaces (e.g., telecommuting, alternative duty station, on travel, etc.).

### 1.2.1 Management Responsibilities

Managers grant users access to agency resources that are within their area of authority. In addition to the expectations that apply to all users granted access to agency resources, managers have additional responsibilities:

1. Ensure that all users have read, understood, and agreed to follow these rules of behavior.
2. Ensure that all new hires receive mandatory security awareness training, and that users with significant security responsibilities receive pertinent role-based security training within the specified timeframe as described in [ISP 3.2 Awareness and Training](#)
3. Ensure that users obtain adequate corresponding training prior to systems access.
4. Restrict systems access to the minimum level required to perform assigned duties.
5. Ensure proper personnel screening is conducted prior to allowing personnel access to any SSA systems with special privileges.
6. Periodically review and validate the permissions assigned to user accounts.
7. Take appropriate action on all reported violations and suspected violations.
8. Ensure that all users have received adequate instruction, training, and supervision regarding users' responsibilities for safeguarding Personally Identifiable Information (PII) and other sensitive information (See [ISP 3.3.2.4 Definitions](#)).

### 1.2.2 User Responsibilities

#### 1.2.2.1 Accountability

- Comply with current information security, privacy, and confidentiality practices.
- Behave in an ethically, informed, and trustworthy manner.
- Choose passwords that comply with SSA's password policy, located in [ISP 3.1 Access Control](#).
- Be accountable for all transactions issued in connection with their account credentials.

- Never share their password with anyone. It is a security violation resulting in disciplinary actions against both parties.
- Have formal authorization from their supervisor (or other specified management official or representative) before accessing sensitive or critical applications.
- Only use their access for the performance of their official duties.

#### **1.2.2.2 Integrity**

- Never intentionally enter unauthorized, inaccurate, or false information.
- Never expose critical data or sensitive information to conditions that may compromise the data's integrity.
- Review the quality of information as it is collected, or generated to ensure that it is accurate, complete, and up-to-date.
- Take appropriate training before using a system, in order to minimize the potential for errors.

#### **1.2.2.3 Confidentiality**

- Disclose information obtained in the performance of their duties only as described in the policy and procedures for that system.
- Take precautions to eliminate viewing by unauthorized parties.
- Log-off or lock workstations when leaving devices unattended.

#### **1.2.2.4 Awareness and Training**

- Be alert to any indicators of system abuse or misuse.
- Complete the mandatory Information Security Awareness Training within the specified timeframe as described in ([ISP 3.2 Awareness and Training](#)).
- Participate in all required Information Security training and awareness ([ISP 3.2 Awareness and Training](#)) activities as identified by management or required by policy.

#### **1.2.2.5 Sensitive Information**

- Protect all sensitive information whether officially on duty or not on duty, at their official duty station, another official work location, or an alternate duty station (See [ISP 3.3.2.4 Definitions](#) for classes of sensitive information).
- Agree to follow the guidance in the Administrative Instructions Manual System, General Administration Manual, [Chapter 15](#), PII Loss and Remediation regarding PII.
- Protect Controlled Unclassified Information (CUI) in accordance with the agency's [CUI Policy](#).

#### **1.2.2.6 Hardware, Software, and Copyright Protection and Control**

- Only use SSA systems resources purchased through the agency-sanctioned requisition procedures or software that has been developed, evaluated, documented, and / or

distributed in-house. More information is located in, ([ISP 2.1.2 Authorized Hardware & Software](#)) Hardware, Software and Platform Configuration Policy.

- Do not disable any SSA security features unless authorized by management.
- Use only approved SSA systems resources. Connecting personally owned hardware, software, and media to SSA systems resources is prohibited (See [ISP 2.1.2](#) and [ISP 3.6.3](#) for exceptions).
- Take necessary precautions to protect SSA's equipment, laptops, and other Portable Electronic Devices (PED) against loss, theft, damage, abuse, or unauthorized use by employing appropriate protection measures.
- Protect copyright information in accordance with the conditions under which it is provided and Federal copyright laws.
- Do not make illegal copies of software.
- Follow SSA's policy on limited personal use of government [office equipment](#).
- Comply with all SSA policy and procedures regarding the use of e-mail, as well as other forms of electronic communications [ISP 3.3.5](#)
- Properly safeguard removable media.

#### **1.2.2.7 Alternative Worksite (Non-SSA Controlled Locations)**

- Follow the security and safety requirements of an alternative worksite agreement. If operating without such an agreement, ensure that all SSA security and safety policies are applied.
- Adhere to all rules of behavior requirements while at the alternative worksite.
- Do not print any material that contains PII at an employee's Alternate Duty Station (ADS).
- Safeguard and properly dispose of any other sensitive printed material.

#### **1.2.2.8 Public Disclosure**

- Employees must follow [SSA's Social Media Policy](#) when using social media web sites for both official business and personal use. Additionally, employees authorized to use social media in an official capacity for the agency must follow the mandatory guidance outlined in [SSA's Social Media Management Policy](#).
- Ensure the appropriate SSA management officials approve SSA information available through public access channels for public dissemination. Consult with the Office of Communications (OCOMM) regarding approved methods for publicly disseminating official agency information.
- Never transmit, store, or process sensitive or proprietary SSA information on external sites, unless explicitly authorized to do so. This includes social media, online forums, third-party collaboration tools or sites, social networking sites, and any other non-SSA-hosted sites, including unapproved third-party data storage providers.
- Do not share programming code used for SSA information systems with unauthorized individuals. This includes, but is not limited to, posting code to unauthorized online

forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.

### **1.2.2.9 Incident Reporting**

- Report suspected virus attacks, malicious / unauthorized intrusion or access in accordance with [ISP 4.1.3 Reporting](#).
- Report suspected violations of the Social Security Act, Privacy Act and other laws, as well as SSA policies and procedures to management in accordance with [ISP 4.1.3 Reporting](#).

### **1.2.3 Consequences of Rules Violations**

In those instances where users do not follow the prescribed rules of behavior or violate other agency information security policies, supervisors may enact penalties enforceable under existing policy and regulations ranging from verbal and official written reprimands through suspension of system privileges, temporary suspension from duty, removal from current position, to termination of employment, and possible criminal prosecution. The specific discipline imposed shall be determined on a case-by-case basis, taking into consideration the nature and severity of the violation, prior violations of the policy committed by the individual, state and federal laws and all other relevant information.

Supervisors should understand that they also may be subject to disciplinary action for their failure to take appropriate action upon discovering a policy violation, such as a breach, or their failure to take required steps to prevent a policy violation from occurring, including adequately instructing, training, and supervising employees regarding their responsibilities for protecting the agency's Information Technology (IT) resources and data.

The [Agency Policy](#) for Systems Access, Table of Penalties for Violations and Acknowledgements Statement by Employee provides further information on consequences for unauthorized systems access. Additional information can be located in the [Code of Federal Regulations](#).

## 2 Section II: Identify

This section provides Information Security policy for managing cybersecurity risk to systems, assets, data, and capabilities. It includes the following categories:

- Asset Management (ID.AM);
- Business Environment (ID.BE);
- Governance (ID.GV);
- Risk Assessment (ID.RA); and Risk Management (ID.RM);

### 2.1 Asset Management

The following subsections provide SSA's policies related to Asset Management. The objective is to ensure that data, personnel, devices, systems, and facilities that enable SSA organizations to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

#### 2.1.1 Platform Boundary

A Computing platform is the environment on which computer programs can run. This may include a computer architecture, an operating system (OS), or runtime libraries. Platforms may also include hardware, firmware, a traditional operating system, or Cloud-based Platform-as-a-Service solutions. A Platform Boundary is a collection of identical or nearly identical Platforms, to which Controls are applied consistently. The Information System Boundary inherits many of these Controls. The Office of Information Security (OIS) publishes and maintains a list of Authorized Platforms, as well as Security Configuration Standards for each of those Platforms.

#### 2.1.2 Authorized Hardware and Software

SSA authorized hardware or software must be:

- On the [authorized hardware list](#).
- On the [authorized platforms list](#).
- On the [authorized desktop software list](#)
- On the authorized [server software list](#).
- Permitted through a documented [approved exception](#).

**NOTE**

*No Kaspersky branded products are to be used, as per DHS Binding Operational Directive.*

At an employee's Alternate Duty Station (ADS), only personal keyboards, monitors, docking stations and mice may be used with the following restrictions:

- The interactive installation of unauthorized drivers or other software on an SSA-imaged machine is prohibited. To determine whether a device requires the interactive installation of unauthorized drivers, see [Unauthorized Drivers](#).
- Devices with Internet capabilities or data storage capacity are prohibited from connecting to SSA owned resources.

All installed software or hardware must follow [security configuration standards](#).

SSA assets must be registered using the SSA-authorized asset manager solutions.

#### **2.1.2.1 Remediation**

The Office of the Deputy Commissioner for Systems (ODCS) must perform regular scans of the network. If unauthorized hardware or software is found, it may be removed without notice. Users who have installed unauthorized hardware or software may face disciplinary action.

#### **2.1.3 Information System Boundary**

An Information System Boundary is a collection of endpoint devices (any device that communicates on SSA's network) that support an Information System. Information System Boundaries can be grouped into subordinate system boundaries.

[Information Systems](#) must be grouped into Information System Boundaries in accordance with the [Cyber Risk Management Strategy](#). All Information Systems must maintain a real-time inventory of Endpoint Devices that form that Information System, as required by SSA's Information Security Continuous Monitoring (ISCM) Strategy. Endpoint Devices may support more than one Information System, but in those circumstances, Controls applicable to those Information Systems will be assessed for effectiveness.

#### **2.1.4 IT Systems and Inventory**

SSA has developed, and maintains a current inventory of IT Systems, as required by the Federal Information Security Modernization Act of 2014 (FISMA) and the Paperwork Reduction Act Section 3505. OIS works with all the relevant components to ensure the agency has a current inventory and policy supporting that inventory. For additional references, see [Enterprise Architecture \(EA\) Inventory Policy – Management of the Enterprise IT Inventory](#).

SSA's major IT Systems have been rated and assigned an impact level per NIST Federal Information Processing Standard (FIPS) 199. SSA systems process and store "sensitive"

information and are required to implement the security controls provided by NIST SP 800-53, Rev. 4 for the corresponding impact level.

When the Project Scope Agreement (PSA) for a developing system process is being created, it is the Systems Project Manager (SPM) and Business Project Managers' (BPM) responsibility to determine where the developing process "fits" in the current agency system architecture. Such as:

- Is this a new system that would have to complete Security Authorization Processes on its own?
- Is this a process that would qualify as a subsystem of an existing system?
- What additional risk(s) will the new process/application have on the current architecture?
- How will the new system/application/etc...affect the overall security posture of the agency (e.g. High system, moderate)?

These are questions that must be answered as the PSA is being completed. The SPM and BPM must meet with the Security Authorization Manager (SAM) of the system within whose security authorization boundary the new system must operate. It is also the BPM and SPMs' responsibility to see that the system development process follows the guidance detailed out in the Systems Development Life Cycle (SDLC) on (b) (7)(E). This includes ensuring the security tasks (SSPs, Security Controls Testing, and Risk Assessments) in the life cycle process are carried out.

OIS may be contacted as a consultant during this process. If there is no established Security Authorization for the new process, OIS should be notified as early as possible in the development of the system.

### 2.1.5 Information System Interconnections and Information Flow

For each persistent interconnection to an external system (such as a Virtual Private Network (VPN)), the Authorizing Official (AO) must approve the connection through an [Interconnection Security Agreement \(ISA\)](#) or other document that contains the necessary NIST SP 800-47 "Security Guide to Interconnecting Information Technology Systems" requirements.

### 2.1.6 Security Categorization and Prioritization

SSA data, and information derived from data, are sensitive and vary in level of sensitivity, dependent on its specific utility and the potential impact of an unauthorized disclosure. Security controls are selected and implemented based on the potential impact that a loss of confidentiality, integrity, or availability would have on operations, assets, and/or individuals associated with SSA.

[FIPS Publication 199](#) defines three levels of potential impact:

Potential Impact	Definitions
------------------	-------------



Low	The potential impact is low if – The loss of confidentiality, integrity, or availability has a limited adverse effect on organizational operations, organizational assets, or individuals
Moderate	The potential impact is moderate if – The loss of confidentiality, integrity, or availability has a serious adverse effect on organizational operations, organizational assets, or individuals
High	The potential impact is high if – The loss of confidentiality, integrity, or availability has a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

All systems must be categorized in accordance with FIPS 199, based on the type of data processed by the information system and the system categorization level.

### Identifying and Prioritizing Critical Resources

The identification and prioritization of [critical resources](#) is necessary to determine which resources require priority in the planning and disaster recovery process. Each component must identify critical resources of their operation. Senior management must determine the agency-wide critical resources and priorities. The Commissioner approves these priorities prior to inclusion in the Disaster Recovery Plan ([DRP](#)). The Office of Systems uses those priorities as a basis for determining the systems resources required in case of a disaster, and in planning for providing those resources. This process is a part of the [vulnerability assessments](#) required for Continuity of Operations ([COOP](#)), which are necessary prior to the development of Contingency Plans or DRPs. Contingency planning for information resources requires planning for five types of resources:

- Processing capability
- Computer-based services
- Data and applications
- Systems operations and support personnel
- Physical resources required to continue systems operations

**NOTE**

See [Section 2.2.2](#) for more information on Contingency Planning



## 2.1.7 CyberSecurity Roles and Responsibilities

The following components or groups have specific cybersecurity responsibilities. A comprehensive list of roles and responsibilities is included in Appendix A of this document.

- The Office of Information Security (OIS):
  - Supports the agency’s Chief Information Officer(CIO) and the Chief Information Security Officer (CISO) in carrying out the information security responsibilities required by FISMA and other related laws, regulations, and standards.
  - Maintains a comprehensive, agency –wide information security program of controls that protect our information and communication assets.
  - Provides criteria determining the frequency of access control reviews.
  - Is responsible for cybersecurity policy and oversight.
  - Approves all standards and procedures for logical system access.
  - Detects attacks, identifies suspicious activities, and systematically responds to software and hardware vulnerabilities as identified.
- Information Security Officers (ISOs) implement the agency’s Information Security Policies and Procedures, Access Control Administration, Security Compliance Monitoring, and Security Awareness. For full descriptions of ISO functions see the [ISO Manual](#).
- SSA Managers or their designees must:
  - (b) (7)(E) certify authorized logical access for [redacted], business partners, agents, and any other individual operating on behalf of the SSA (b) (7)(E) [redacted]
  - Approve and monitor appropriate hours of access for their component.
    - The immediate manager is responsible for approving hours of access for his or her employees.
    - Management must periodically review the appropriate hours of access for their employees.
  - (b) (7)(E), (b) (2) [redacted]
  - (b) (7)(E), (b) (2) [redacted]
  - This policy allows flexibility for managers to adjust the hours according to the specific needs of an office.
- Notify SAM of significant changes in a user’s logical access requirements (i.e., when users will not need to access the system due to extended leave or suspension, are transferred to another component, or leave the agency).

- Network Administrative staff (e.g., Site LAN Coordinator (SLC) / Local Area Network (LAN) Administrator, etc.), under the direction of the local manager, and often working in conjunction with OSOHE:
  - Monitors user accounts and activity to ensure access to the network is appropriately limited and consistent with business needs defined by management.
  - Implements LAN security standards at the local site.
  - Ensures each user is aware of the minimum security requirements to operate effectively within the LAN environment, and with the understanding that non-compliant devices may be restricted from network connectivity.
  - Ensures all LAN configurations uniquely identify and authenticate all user credentials when presented to an Information System.
  - Ensures the efficient and technical operation of the SSA e-mail systems and maintain the integrity and confidentiality of the e-mail messages (SLCs may not read user e-mail messages unless specifically directed to do so by authorized management officials).
  - Reports incidents to the National Network Service Center (NNSC) and notify their CDSI / CSO.

## 2.2 Business Environment

The following sections provide policy to ensure that the SSA mission, objectives, stakeholders, and activities are understood and prioritized. This information is also used to inform cybersecurity roles, responsibilities, and risk management decisions.

### 2.2.1 Supply Chain Risk Management

SSA manages potential risks associated with information and communications technology (ICT) products and services in accordance with [NIST SP 800-161, \*Supply Chain Risk Management Practices for Federal Information Systems and Organizations\*](#).

During initial stages of the procurement of IT products or services, OAG works with OIS to determine whether a Supply Chain Risk Assessment (SCRA) is required for the procurement based on a set of predefined criteria.

For details, please refer to the [Supply Chain Risk Assessment Guidelines](#) document.

### 2.2.2 Contingency Planning

This section identifies the agency's planning principles and practices for developing and maintaining effective contingency plans. It also provides guidance to assist personnel in evaluating Information Systems, and operations, in order to determine contingency planning requirements and priorities. This section presents a structured approach to aid planners in

developing cost-effective solutions that accurately reflect their IT requirements, and in integrating contingency planning principles into the System Development Life Cycle (SDLC) process.

Contingency planning refers to interim measures to recover Information Technology (IT) services following an emergency or system disruption. Course of action may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods.

SSA has various security controls in place to protect the agency's information from alteration, destruction, loss, or disclosure. Malicious attackers attempt to gain access to SSA systems in a variety of forms. For additional information, see [Office of Information Security \(OIS\) Incident Response page](#).

In order for contingency planning to be successful agency management must:

- Understand the IT contingency planning policies and incident response plans have emphasis on maintenance, training, and exercising the contingency incident response plan.
- Understand the Contingency Planning (CP) Processes and their place within the overall Continuity of Operations Plan and Business Continuity Plan process.
- Annually examine the contingency and incident response policies and include the elements: preliminary planning, business impact analysis, alternate site selection, and recovery strategies.

Contingency Planning and Risk Response encompasses all Information Systems administered by SSA or on behalf of SSA, hosted on and / or off premises, including agency-approved [Cloud Service Providers \(CSP\)](#).

### **2.2.2.1 Information System Contingency Planning**

The purpose of the Information System Contingency Plan (ISCP) is to describe interim measures to recover Information System services after an adverse effect to operations. Contingency planning establishes a thorough plan, procedure, and technical measures that can enable the recovery of information systems after a disruption. The SSA Information System Owner (SO) and Security Authorization Manager (SAM) must document Business Impact Analysis (BIA) considerations as part of the contingency planning process to determine and evaluate the potential effects of an interruption to critical business operations. The BIA is then used to develop and maintain the ISCP according to the [ISCP standards document](#).

As part of the contingency planning process, Information SOs and SAMs for SSA Information Systems must:

- Complete a BIA.

- Determine the level of detail required in the ISCP in accordance with [NIST 800-34, Rev 1](#) and the [SSA ISCP Standard](#).
- Develop and maintain a list of key contingency personnel that includes names, roles, and responsibilities.
- Complete and ensure copies of the approved ISCP are distributed to listed key contingency personnel.
- Ensure contingency plans are updated at least annually.
- Communicate ISCP changes to the listed key contingency personnel.
- Train personnel in their contingency roles and responsibilities with respect to the Information System and provide annual refresher training. Test and / or exercise the ISCP for the Information System at least annually to determine the plan's effectiveness, and the organization's readiness to execute the plan. See [NIST SP 800-34, Rev 1](#) for guidance on designing, developing, conducting and evaluating test, training and exercise events.

The following contingency planning policies are applicable to all SSA Information Systems. Information SOs and SAMs for SSA Information Systems must:

- Maintain a list of key contingency personnel that includes names, roles, and responsibilities.
- Ensure copies of the approved ISCP are distributed to listed key contingency personnel.
- Review and update the ISCP annually, based on current threat information, or when major changes occur to the system.
- Communicate changes from the ISCP to the listed key contingency personnel.
- Train personnel in their contingency roles and responsibilities with respect to the Information System and provide annual refresher training.
- Test and / or provide exercise for the ISCP for the Information System at least annually to determine the plan's effectiveness, and the organization's readiness to execute the plan.

#### **2.2.2.2 Contingency Planning Policy**

The Contingency Planning Policy includes:

- Developing a [Continuity of Operation Plan \(COOP\)](#) to ensure that the agency's mission critical functions can continue to operate after a disaster;
- Developing and testing a Contingency Plan (See [ISP Section 2.2.2.1](#));
- Reporting and correcting any system security weaknesses discovered in the Contingency Plan through risk analysis or audit reviews of a sensitive application;
- Conducting periodic security assessments (at least annually) to ensure all continuity operation procedures are up-to-date;
- Developing a backup plan for all critical applications and assets that includes:
  - Securing a backup storage facility (onsite and offsite);

- Ensuring that contracts for any offsite storage facilities follow all security policies for safeguarding and protecting Agency assets; and
- Testing backup plan procedures periodically to ensure that information is retrievable and available.

The above requirements are consistent with Department of Homeland Security (DHS) Presidential Directive HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection. The resulting plans are an important component of SSA's COOP, which is developed in compliance with the HSPD-6, Enduring, Constitutional Government and Continuity of Government Operations, OMB Circular A -130, and FISMA.

Contingency planning for SSA's Information Systems is a part of the agency's Critical Infrastructure Protection (CIP) process. As such, many of the steps required for contingency planning complete a part of developing and updating the agency's COOP. The following considerations address specific IT assets and their relationship to the SSA [Emergency Management Program and COOP](#).

## 2.3 Governance

### 2.3.1 Information Security Policy

SSA takes a responsible, cost-effective, approach to Information Security. Information security requires the implementation of reasonable controls identified as representing sound security practices. The Office of Information Security The Information Security Policy (ISP) is SSA's overarching security policy where FISMA requirements are translated and applied agency wide. (b) (7)(E). These requirements balance operational and service delivery with security conditions to ensure personal data entrusted to SSA is not compromised, abused, or misused by the public or SSA employees.

To meet the security policies requirements SSA develops and maintains the following types of documents:

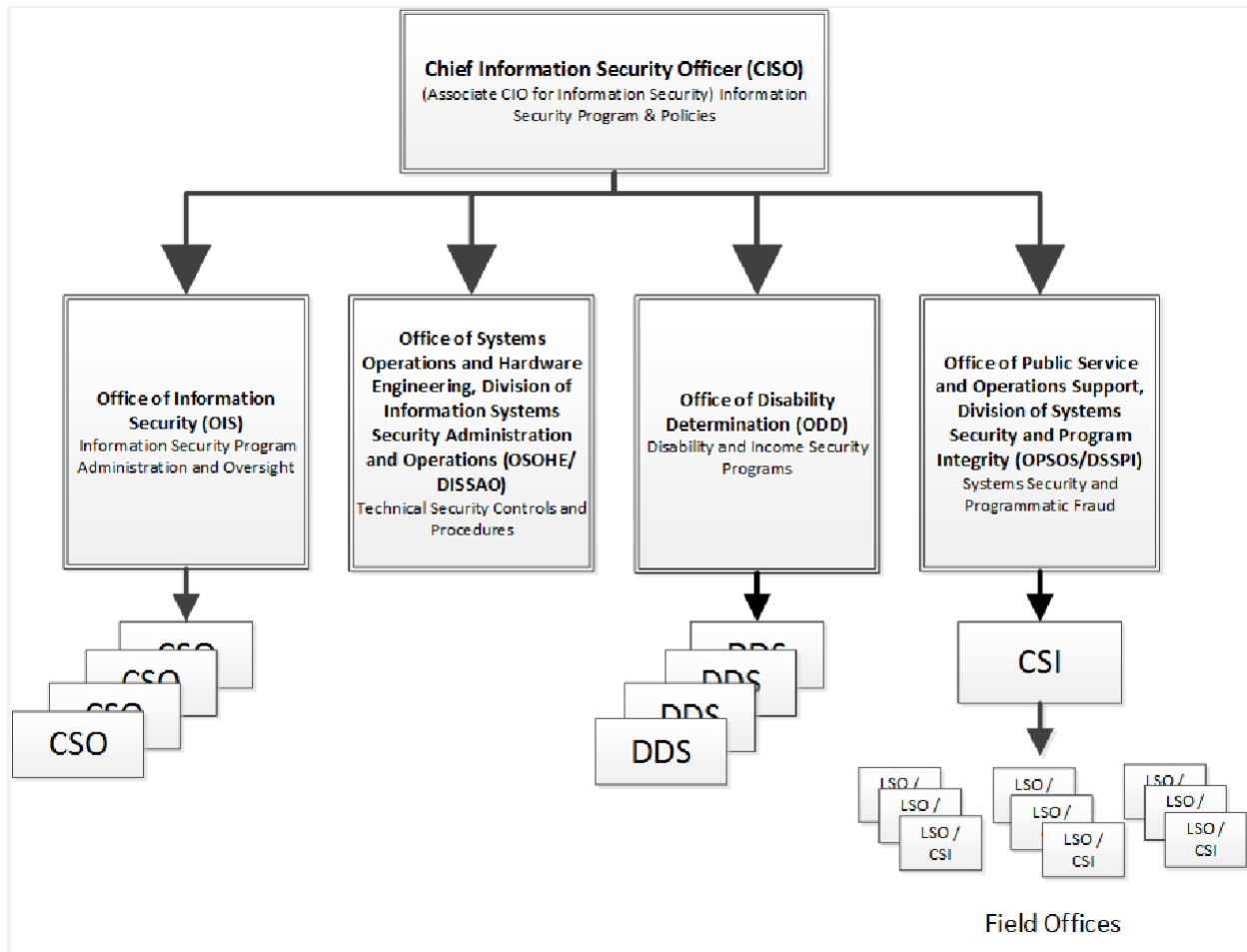
- **Policy** – High-level statements of what must be done, based on law, rules, regulations and agency directives.
- **Standards** – Published statements, or requirements, specifying characteristics that must be satisfied or achieved in order to support individual policies.
- **Guidelines** – General statements for accomplishing a specific task or implementing a procedure.
- **Procedures** – Mandatory, systematic, detailed actions, required to complete a task or achieve a specific outcome.
- **Process** - A series of procedures or events to accomplish a result.

### 2.3.2 Security Organization Structure

The SSA Chief Information Security Officer (CISO) oversees the Information Security program and policies. Key organizational components with responsibilities within SSA's Information Security program are as follows:

- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)

SSA CONFIDENTIAL INFORMATION



Roles and Responsibilities for Cybersecurity personnel are provided in Appendix B.

### 2.3.3 Laws and Regulations

SSA is subject to statutory requirements to protect the sensitive information it collects and maintains on individuals. SSA establishes administrative controls to prevent fraud, waste, and abuse. These statutory requirements are contained in the following documents:

- [Internal Revenue Service \(IRS\) Tax Information Security Guidelines for Federal, State and Local Agencies \(2014\).](#)
- [FISMA.](#)
- [The Clinger-Cohen Act \(CCA\) of 1996.](#)
- [Freedom of Information Act \(FOIA\) of 1996.](#)
- [Office of Management and Budget \(OMB\) Circulars A-123 \(1995\), A-127 \(2009\), and A-130 \(1996\).](#)
- [Federal Managers' Financial Integrity Act \(FMFIA\) of 1982.](#)
- [Records Management by Federal Agencies \(44 U.S.C. Ch. 31, 1976\).](#)

- [Privacy Act of 1974](#).
- [E-Government Act of 2002](#).
- Federal Information Processing Standards (FIPS) [199](#) and [200](#).

SSA takes a responsible, cost-effective, approach to Information Security. Information security requires the implementation of reasonable controls identified as representing sound security practices. (b) (7)(E)

These requirements balance operational and service delivery with security conditions to ensure personal data entrusted to SSA is not compromised, abused, or misused by the public or SSA employees.

## 2.4 Risk Assessment

### 2.4.1 Security Assessment and Authorization (SA&A)

[OMB Circular A-130](#), and [FISMA](#) require that all Federal agencies institute an agency-wide Information Security program to provide Information Security for the information and Information Systems that support the agency's operations and assets. This includes those systems provided or managed by another agency, contractor, or other source.

#### 2.4.1.1 The SSA Risk Management Framework (RMF) Process

The System Owner (SO) is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. All SSA SOs must institute a comprehensive assessment of the management, operational, and technical security controls in an Information System, to ensure that Information System-related security risks are being adequately addressed on an ongoing basis; and the authorizing official explicitly understands and accepts the risk of organizational operations and assets, individuals, and other organizations.

At SSA, the information SO is a senior Agency official at the Associate Commissioner level, or equivalent. The Information SO may delegate their information system owner responsibilities in writing to the SSA CISO. Delegates must have appropriate authority to complete the information SO responsibilities.

SSA's [Security Assessment and Authorization Process](#) applies the six (6) distinct steps of the [Risk Management Framework](#), as explained in [NIST SP 800-37, Rev. 1 – "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach"](#):

Categorization of Information and Information Systems:

- Select Security Controls
- Implement Security Controls



- Assess Security Controls
- Authorize Information Systems
- Continuous Monitoring

See the Security Assessment & Authorization Process website for more detailed guidance.

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

The System Security Plan (SSP) is required. The SSP provides an overview of the information system security requirements and describes the security controls in place or planned. The security safeguards implemented for the information system must meet the policy and security control requirements identified in the SSP.

It is imperative that the plan is current so that an accurate picture of the system is always available. (b) (7)(E)

See [Section 7.2 Appendix B: Roles and Responsibilities – Security Authorization Manager \(SAM\)](#) for more information.

The SSP must be consistent with the guidelines in [NIST SP 800-18, Rev. 1, Guide for Developing Security Plans for Federal Information Systems](#), and the security controls in the security plan must be consistent with [FIPS 199 – Standards for Security Categorization of Federal Information and Information Systems](#), [NIST SP 800-60, Volume 1, Rev. 1 – Guides for Mapping Types of Information](#) and [NIST SP 800-60, Volume 2, Rev. 1 – Information Systems to Security Categories](#).

#### **2.4.2 Threat and Vulnerability Management**

Vulnerabilities detected through various assessments must be tracked and mitigated according to the [Penetration Testing Tracking and Remediation Process](#). OIS tracks and monitors the remediation of findings and other discovered vulnerabilities to ensure that they are mitigated in accordance with the agency's remediation timeline.

#### **2.4.3 Information System Risk Assessment**

All systems created by SSA must incorporate the Risk Management Framework (RMF) as identified in [NIST SP 800-37, Rev. 1](#). The applicable systems include:

- Systems used within any part of SSA.
- New systems (Internet, intranet, client / server, non-Internet / Applications, collaborative systems, standard development, and others).
- Modifications to existing systems.
- Systems developed in the Office of Systems (OS) or in any other SSA component.
- Systems developed by contractors and Commercial Off-the-Shelf (COTS) or Government Off-the-Shelf (GOTS) products.

A majority of system development at SSA follows the SDLC maintained by the Office of Systems on (b) (7)(E) includes specific security considerations throughout the SDLC process that associates to the RMF. The System Owner (SO) must ensure all elements of the RMF are followed.

### Project Resource Guide (b) (7)(E)

The official SDLC roadmap that SSA follows when it develops software tools or applications is available on (b) (7)(E) This includes requirements development, appropriate timeframes, and sample template documents. SDLC related security considerations on (b) (7)(E) include, but are not limited to:

- System categorization and asset identification,
- Initial security risk assessment,
- Security requirements development,
- Security planning and control development,
- Security control integration,
- Final security risk assessment,
- Security Assessment & Authorization (SA&A),
- Configuration and change control
- Continuous monitoring and risk assessment updates.

For existing systems, the risk assessment process must be performed at least every three (3) years for all enterprise level Federal Information Systems. (b) (7)(E)

- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)

The SSA Risk Management Program is developed to satisfy the following security objectives:

- **Confidentiality** – Protection from unauthorized disclosure (see [FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004](#), for more information on Confidentiality).
- **Integrity** – Protection from unauthorized, unanticipated, or unintentional modifications. This includes, but is not limited to:
  - Authenticity – A third party must be able to verify that the content of a message has not been changed in transit.
  - Non-repudiation – The origin or the receipt of a specific message must be verifiable.

- Accountability – A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity (see FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004, for more information on Integrity).
- **Availability** – IT resources (system or data) must be available on a timely basis to meet mission requirements or to avoid substantial losses. Availability also includes ensuring that resources are used only for intended purposes (see FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004 for more information on Availability).

PMs and SAMs are required to follow the risk assessment process to determine the potential threats and risks associated with developing / revising systems. The output of the process should help identify appropriate security controls to mitigate risks. The process must include documenting and close monitoring of any residual risks.

#### **2.4.4 Additional Information**

Federal information is a strategic asset subject to the risks that must be appropriately managed to minimize harm. The level of risk is determined by the likelihood that a threat event will occur and result in adverse impact to an IT system or business processes. Agencies use risk assessments to determine the impact and likelihood of risks associated with an IT system (or data) throughout the SDLC. The output of this process helps identify appropriate controls for reducing or mitigating risk during the risk mitigation steps

For detailed description on the Risk Management Framework, see NIST SP 800-37, [“Guide for applying the Risk Management Framework to Federal Information Systems”](#).

In addition, SSA approaches risk management by using Federal guidelines provided for risk assessment in NIST SP 800-30, [“Guide for conducting Risk Assessments”](#).

## **2.5 Risk Management Strategy**

This section provides policy to ensure that the organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

### **2.5.1 Risk Management**

[OMB Circular A-130](#), and [Federal Information Security Modernization Act of 2014](#) (FISMA) require that all Federal agencies institute an agency-wide Information Security program to provide Information Security for the information and Information Systems that support the agency’s operations and assets. This includes systems provided or managed by another agency, contractor, or other source.

SSA’s policy for Information Security Risk Management is the practice of identifying, prioritizing, and estimating risks that threaten the confidentiality, availability, and integrity of

information, and the associated SSA Information Systems. Identifying vulnerabilities and developing safeguards increases awareness of security concerns by involving all components responsible for the development of the application in the process.

The policy reviews requirements and guidelines for SSA's internal controls (audit trail system and integrity review process), along with additional Information System audit coverage areas (System and Application). Internal control requirements to protect sensitive information are electronically stored on or transmitted by SSA's Information Systems. Policy requirements for implementation of effective technical, operational and management controls are made to prevent, determine and detect improper payment and improper disclosure. Moreover, the policy requirements and guidelines provided in this section facilitate investigation in circumstances of potential improper payment, improper disclosure, fraud, and abuse.

In addition, the Risk Management section establishes SSA security guidelines for Web application development, in order to ensure confidentiality, integrity, and availability for collecting, disseminating, and transmitting SSA-sensitive information via the agency's network. The guidelines comply with both Federal regulations and business requirements

Project Managers (PMs) must follow appropriate risk assessment methodology as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach; NIST SP 800-30, rev. 1, Guide for Conducting Risk Assessments; and NIST SP 800-39, Managing Information Security Risk: Operation Mission, and Information System View.

Risk Management of IT Systems encompasses all Information Systems and Automated Information Systems (AISs) administered by SSA or on behalf of SSA, hosted on and / or off premises, including agency-approved Cloud Service Providers (CSP).

### 3 Section III: Protect

This section provides the policy for developing and implementing safeguards to ensure delivery of SSA services. It includes the following categories:

- Access Control; (PR.AC)
- Awareness and Training Data (PR.AT) ;
- Data Security (PR.DS);
- Information Protection Processes and Procedures (PR.IP);
- Maintenance (PR.MA); and
- Protective Technology (PR.PT)

#### 3.1 Access Control

The Information Security Policy (ISP), along with other supporting standards and procedures, establishes the basis for implementing secure access controls for the Social Security Administration's (SSA) Information Technology (IT) resources and associated Information Systems, and ensuring access to assets is limited to authorized users, processes, or devices, and to authorized activities and transactions.

Access Control encompasses all Information Systems administered by SSA, or on behalf of SSA, hosted on and / or off premises, including agency-approved [Cloud Service Providers \(CSP\)](#).

##### 3.1.1 Identity and Credential Management

SSA's logical access policy complies with the Federal Information Security Modernization Act of 2014 (FISMA) and mandated controls described by the National Institute of Standards and Technology (NIST) and the Chief Information Officer (CIO) Council's Federal Identity, Credential, and Access Management (FICAM) initiative mandated by the Office of Management and Budget (OMB).

All Information System roles associated with access management administration and maintenance (e.g., Manager, Security Officer, Network Administrator, Contracting Officer Representative (COR), etc.) use the SSA's standards and procedures listed below for administering and maintaining logical access to SSA's Information Systems:

- The [Security and Access website](#) provides the standards and procedures for managing identities, credentials, and access (e.g., (b) (7)(E), (b) (2)

- The [Information Security Officer \(ISO\) Manual](#) contains additional actions for Security Officers to perform their responsibilities related to access control management

### 3.1.1.1 Identity Management

A digital identity permits access to SSA's Information Systems. To obtain access to SSA's Information Systems, individuals must first undergo the Personal Identity Verification (PIV) process that is mandated by Homeland Security Presidential Directive (HSPD) 12, in accordance with applicable guidance set forth in OMB M-05-24 and Federal Information Processing Standards (FIPS) 201-2. For further information regarding the policy for the agency's PIV process, see Personal Identity Verification and Credential Issuance Process.

For all agency Information Systems, each Information System Manager must follow SSA's established procedures to grant environmental access and administer user accounts located on the Security and Access website and in the [Information Security Officer \(ISO\) Manual](#).

All non-SSA employees (contractors and other employees of SSA affiliated agencies) are required to have an SSA-approved written agreement or contract.

The Office of Personnel [Center for Security and Suitability Program](#) is responsible for position designation and determining the suitability of SSA and non-SSA personnel.

### 3.1.1.2 Credential Management

Upon the creation of a digital identity, the following actions are required:

- (b) (7)(E), (b) (2)
- (b) (7)(E), (b) (2)
- (b) (7)(E), (b) (2)
- (b) (7)(E), (b) (2)
  - The creation, activation, modification, and granting of all logical access must comply with the [Information Security Officer \(ISO\) Manual](#):
    - Section 3 Access Control Administration
    - Section 3.6 - Application For Access To SSA Systems
  - For access instructions (personnel / contractors) to SSA platforms, and associated access request forms, see the Security and Access site: Environment Access and Security Forms.
  - (b) (7)(E), (b) (2) All new IT product and service procurements must be compliant with PIV standards and interoperable with agency-issued PIV smart cards.

- Requests for removal of access to Information System accounts and other information resources must adhere to the following:

- (b) (7)(E), (b) (2) [Redacted]
- (b) (7)(E), (b) (2) [Redacted]
- (b) (7)(E), (b) (2) [Redacted]

- (b) (7)(E), (b) (2) [Redacted]
- (b) (7)(E), (b) (2) [Redacted]
- (b) (7)(E), (b) (2) [Redacted]

- (b) (7)(E), (b) (2) [Redacted]
- (b) (7)(E), (b) (2) [Redacted]
- (b) (7)(E), (b) (2) [Redacted]
- (b) (7)(E), (b) (2) [Redacted]

- (b) (7)(E), (b) (2) [Redacted]

The following policy applies to Service Accounts:

- They are site-specific, special-purpose PINs that must be formally approved prior to use in SSA operations.
- They must be used only for running applications or scripts, and must be executed by the system.
- To request a service account or change access for an existing service account, (b) (7)(E), (b) (2) [Redacted]

- These accounts must only be used for the actions approved in the original (b) (7)(E), (b) (2)
- Service Account passwords must adhere to the following criteria:
  - Must be (b) (7)(E), (b) (2)
  - Must meet the standards specified in [SSA's Credential Rules and Requirements](#).
- Service Accounts must be created, established, and maintained with "Non-Interactive Logon". Non-Interactive Logon restricts the ability for an account to logon at a Windows logon screen or a remote desktop session.
  - Exception: Interactive logon may be allowed for Service Account PINs that are managed by the agency's (b) (7)(E), (b) (2)
- Any deviation from the Service Account requirements outlined in this policy must obtain prior approval by submitting a [Request for Exception](#).

### 3.1.1.3 Password Policy

Information Systems must use the appropriate SSA approved credential standard and password rules (Credential Rules and Requirements).

All users must:

- (b) (7)(E), (b) (2)
- Protect their passwords by ensuring they are not displayed, stored, or placed in commonly accessible locations.
- Control their credentials by not sharing their accounts or revealing their passwords with anyone.
- Keep their HSPD-12 credential (PIV smart card) in their possession and not allow others to use it for access.
- Prevent others from using their workstation while logged on with their user credentials.

#### **NOTE**

*This standard excludes authorized SSA technical support employees or contractors who must troubleshoot certain issues, as they may need to perform such work under a user's PIN.*

- Encrypt files that contain passwords.
- Ensure passwords are not stored in readable form (plaintext/unencrypted), in batch files, automatic log-on scripts, software macros, terminal function keys, dial-up communications programs, or other similar locations.



### 3.1.2 Remote Access

The agency documents, monitors, and controls all approved remote access to SSA Information Systems including remote access to privileged applications. The Office of Systems (OS) must provide a secure solution for remote access to authorized users.

In accordance with federal mandates, SSA:

- Limits remote access to approved agency solutions with two-factor authentication (e.g., VPN w/PIV cards).
- Employs automated mechanisms to monitor and control use of approved remote access methods.

Commercial and residential wireless networks (e.g., public hotspots, hotels, home networks), and cellular Internet access are authorized for VPN access to SSANet, provided the following conditions are met:

- SSA-supplied laptop or other mobile devices are used.
- Up-to-date anti-malware signatures and system patches are in place.
- Users do not utilize multi-homing.
- Users are legally authorized to use the network, which is connecting to SSANet.

### 3.1.3 Account Policy

User accounts are segregated into three tiers based on the type of privileges and potential enterprise impact associated with the account.

- (b) (7)(E), (b) (2)
- (b) (7)(E), (b) (2)
- (b) (7)(E), (b) (2)

See the [Account Type Matrix](#) for further clarification on these tiers and the types of accounts associated with them.

Special Consideration by Tier Type:

- (b) (7)(E), (b) (2)
  - (b) (7)(E), (b) (2)

- (b) (7)(E), (b) (2)
- (b) (7)(E), (b) (2)
  - (b) (7)(E), (b) (2)
  - (b) (7)(E), (b) (2)
  - (b) (7)(E), (b) (2)
  - (b) (7)(E), (b) (2)
  - (b) (7)(E), (b) (2)
  - (b) (7)(E), (b) (2)
- (b) (7)(E), (b) (2)
  - (b) (7)(E), (b) (2)
  - (b) (7)(E), (b) (2)

### 3.1.3.1 Access Management

Policy for access management includes the following:

- Privileged accounts must be authorized prior to creation.
  - Individuals user accounts must be authorized by a System Manager (SM) prior to being added to local administrator groups.
- Managers authorize access to SSA Information Systems based upon official business “Need-to-Know,” and limited to the “Least Privilege” access required for performing job functions. Whenever access is granted, it is limited access to those who have a legitimate need for these resources to perform their assigned position responsibilities.
  - The terms “Need-to-Know” and “Least Privilege” express similar ideas.
  - “Need-to-Know” generally applies to people, while “Least Privilege” generally applies to processes (source: [CNSSI-4009](#)).
- System Managers (SMs) must ensure adequate “separation of duties” within the roles of Information Systems.
  - Separation of duties reduces the potential for an individual to abuse authorized access privileges by prohibiting them from controlling all aspects within a process, and bypassing critical controls.

- SMs must establish compensating controls when a conflict in separation of duties is identified. Separation of duties examples include:
  - Dividing mission functions and Information System support functions among different individuals and roles;
  - Conducting Information System support functions with different individuals (e.g., system management, programming, configuration management, quality assurance, testing, and network security);
  - Ensuring security personnel administering access control functions do not also administer audit functions. Security personnel administering audit functions may not perform audit functions for their own activities (source: [NIST SP 800-53](#)).
- Upon suitability clearance, users are authorized access to general SSA network resources. Specific access to information systems necessary to perform job duties must be requested via the agency's [access management platform](#).
- Unauthorized users are prohibited access to Information Systems and must not in any way damage, alter, disrupt, or facilitate the disruption of agency Information Systems operations.
- All information systems must display the agency approved warning banner. The approved banner can be found in the [System Security Baselines](#) for the appropriate platform.
- Accounts must be reviewed periodically to ensure access is appropriate for each user's assigned duties; frequency of review depends upon account type. For more information, see the [Information Security Officer \(ISO\) Manual](#), Sec. 3: "Access Control Administration".
  - (b) (7)(E), (b) (2)
  - (b) (7)(E), (b) (2)
  - (b) (7)(E), (b) (2)
    - (b) (7)(E), (b) (2)
    - (b) (7)(E), (b) (2)
    - (b) (7)(E), (b) (2)
    - (b) (7)(E), (b) (2)
    - (b) (7)(E), (b) (2)
    - (b) (7)(E), (b) (2)
    - (b) (7)(E), (b) (2)
    - (b) (7)(E), (b) (2)
    - (b) (7)(E), (b) (2)

□ (b) (7)(E), (b) (2)

- Account usage must be monitored, and security reports reviewed, according to the procedures in the [ISO Manual](#), Sec. 4.13: “SARA and Top Secret Administration Reports”.
- All Second UserIDs must follow the requirements stated within the [Second User ID Procedures and Audit Process](#).
- Share Access:
  - Agency shared drives must be protected from unauthorized access, modification, data leakage, and disclosure.
  - Only authenticated users with valid SSA approved credentials are permitted to access agency shared drives.
  - Users that create or maintain agency shared drives must explicitly specify users and groups that can access the shared drive, and associated access permissions.
  - Users must not create shared drives on local workstations.
  - Shared drives must be configured in accordance with the agency’s [Share Configuration Requirements](#).

### 3.1.3.2 Systems Access Security Administration

Implementation and management of Security Administration System software are reserved for only authorized SSA staff within the Office of Systems. SSA’s Access Control System and security administration access control software must be compliant to SSA system security policy.

For a system to be in compliance with SSA system security policy must document that it meets the following requirements:

- Reside in the SSA network.
- Enforce SSA policy related to managing users (e.g., (b) (7)(E), (b) (2) ) and performing other security actions and incidents (e.g., logging / audit features, etc.). (b) (7)(E), (b) (2)
- Have encryption capability.
- Have reporting capability.

(b) (7)(E), (b) (2)

### 3.1.3.3 Sanctions for Unauthorized Systems Access

SSA has a published set of uniform sanctions for employee Information Systems access violations. All SSA management officials are responsible for ensuring that these sanctions are enforced in all cases of employee misuse or abuse identified under their jurisdiction. Lead

responsibility for Sanctions for Unauthorized System Access Violations dissemination and enforcement resides with the Deputy Commissioner for Human Resources (DCHR). The purpose of these sanctions is to ensure that any violations of the confidentiality, integrity, and availability of SSA's Information Systems, records are consistent in a manner, that all SSA employees are aware of the consequences of these violations. These sanctions apply to all SSA employees. For more details on these Sanctions and the Acknowledgment Statement, see the [Systems Sanction Policy](#).

### **3.1.4 Network Integrity and Protection**

#### **3.1.4.1 Network Segmentation**

Network segmentation is a method of dividing a network into smaller subnetworks or segments.

Network segmentation must be used to protect High Valued Assets (HVA) and reduce the risk of compromise, data breach and unauthorized network access.

#### **3.1.4.2 Multi-Homing**

Multi-homing is the capability of having concurrent connectivity to the SSA network, and an external network from a computer or network device. Multi-homing is strictly prohibited.

#### **3.1.4.3 Modems in SSA Facilities**

Modems present the possibility of interconnecting computers, and other devices to external networks / systems while bypassing SSA's network security protections. Any modem used in SSA facilities, or connected to SSANet must be authorized by following the modem registration process. (b) (7)(E) must be used for:

- (b) (7)(E)
- (b) (7)(E)

#### **3.1.4.4 Broadband Internet Connections in SSA Facilities**

Off-network broadband Internet connections in SSA facilities allow Personal Computers (PCs) and other devices to connect to external networks / systems while bypassing SSA's network security protections. Also referred to as off-network connections, access to these types of connections includes but is not limited to cable, DSL, and ISDN modems. Use of these connections when there is a business need to access resources may be requested by using the

[Exception Process](#). All off-network connections must be properly registered using the use of Office of Systems Operations and Hardware Engineering (OSOHE) [Registration Procedures](#).

Devices connected to an off-network connection must not be connected to the SSA network (see [ISP Section 3.1.4.2](#) for prohibition on Multi-Homing). No sensitive information may receive, transmit, or store information on devices connected to an off-network connection.

- Devices connected to broadband Internet connections must be configured with security safeguards as referenced in SSA's [security configuration guides](#). It is the requesting component's obligation to maintain adequate security controls on the device.
- All SSA devices that have connected to an external network, including the Internet, must undergo SSA's hard disk wiping procedure prior to connecting to SSANet. **EXCEPTION:** All SSA devices configured in accordance with SSA's standard Virtual Private Network (VPN) configuration may connect to an external network (e.g., public (WiFi), home Internet, etc.) in order to establish a VPN tunnel with SSANet to conduct further Internet-related activities. These devices are not required to undergo SSA's hard disk wiping procedure prior to reconnecting with SSANet information resources.
- The use of off-network connections does not exempt the component or user from meeting agency record retention requirements.
- The local Manager is responsible for monitoring the use of approved off-network broadband Internet connections.

#### **3.1.4.5 Restricted Hardware and Software**

Devices or software designed to scan, analyze, and / or troubleshoot SSA network communications are restricted to use by authorized network and security operations personnel. Unauthorized use of scanning tools and devices is prohibited.

#### **3.1.4.6 Prohibited Security Practices / Activities**

Good security practice requires the protection of sensitive materials, including emails and faxes. Do not leave sensitive materials, Faxes and messages unattended and susceptible to reading by unauthorized individuals.

Individuals who have rights / privileges to view others' e-mail/Faxes are prohibited from doing so unless authorized by appropriate management officials. See

<http://aims.ssa.gov/GAM/G1416.htm> for policy governing how to access an employee's workstation.

### 3.1.5 Limited Personal Use of Government Office Equipment, Including IT

(b) (7)(E), (b) (2)

### 3.1.6 Wireless Technology

The following are allowed for use in SSA's infrastructure, upon enterprise authorization:

- SSA-managed and issued smartphones (including BlackBerry Devices) and cellular telephones;
- Conventional cordless telephones;
- Wireless 'Guest' networks provided they are configured and maintained according to approved security configuration baselines.
- Local managers may approve wireless pointing devices (i.e., mouse, trackball, or keyboards). However, consideration should be given to possible signal cross-talk and interference. Additional guidance on securing these devices can be found in [NIST SP 800-121 Rev. 1, Guide to Bluetooth Security](#).

#### **NOTE**

*An exception must be submitted only if the wireless pointing device requires additional software.*

Employees may use non-SSA wireless networks to connect to SSANet in accordance with the Remote Access Policy.

#### **3.1.6.1 Mobile Computing Devices**

The following applies to mobile computing devices:

- Must be Government Furnished Equipment (GFE).
- Must employ the appropriate agency-approved security configuration.

#### **NOTE**

*SSA's Outlook Web Access (OWA) is an Internet-facing website designed to be accessed via the Internet, and is therefore not subject to these restrictions.*

#### **3.1.6.2 Personally Owned Mobile Computing Devices**

Personally owned mobile computing devices must not connect to SSA network / infrastructure, and must not interfere with SSA's wireless infrastructure.

Exception: Personally owned mobile computing devices may connect to authorized SSA guest wireless networks for business purposes upon authorization and approval.

Personally owned mobile computing devices are permitted for use in non-restricted areas.

### **3.1.6.3 Prohibited Wireless Technology**

The following wireless technology is prohibited:

- (b) (7)(E), (b) (2)
- (b) (7)(E), (b) (2)
- (b) (7)(E), (b) (2)

### **3.1.6.4 Wireless Exception**

Any use of non-compliant wireless technology or wireless devices requires an approved exception (See [Exception Request Process](#)).

- A request for exception must provide a business justification for the use of the wireless technology, the controls planned to limit the associated security risks, and formal acceptance, by the requesting Manager / Director of the residual risks.
- The SSA Chief Information Security Officer (CISO) maintains final approval authority.
- It is acceptable to request exceptions for a group of devices instead of multiple instances, provided these devices are used in an identical manner.

## **3.1.7 Web Services Security**

### **3.1.7.1 Background**

A Web Service, as defined by NIST, is a software component or system designed to support interoperable machine or application-oriented interaction over a network and is sometimes called an application service or microservice. Web Services can be impleted with a range of technologies (e.g. Representational State Transfer (RESTful) or Simple Object Access Protocol (SOAP)).

If authentication is required, authentication processes must ensure that the sender and recipient of the data are known to each other.

- Data access controls incorporates entities or users authorized to send and receive information. According to OMB Memorandum 06-16, dated June 23 2006, transmission of sensitive information using the Internet is permissible as long as an acceptable method of encrypting the confidentiality and integrity of the information.



- For encryption requirements, see ([ISP Section 3.3.1, Protection of Information in Transit and at Rest](#)).
- The System Owner (SO) is responsible for determining the need for digitally signing messages. When required, all digital signatures must use NIST-compliant cryptography.
- Clients must authenticate using NIST-compliant asymmetric cryptographic cryptography (e.g., PKI certificates or Javascript Signing and Encryption (JOSE) public/private keypairs).
- For keys presented to authenticate clients, SSA must be able to establish trust with the issuer and support revocation.
  - If a key is fraudulently used, the issuer is no longer valid, or at the request of the CIO or CISO, keys must be disabled for use with SSA services.
- Access controls for entities and affiliates must follow the requirements specified in [Section 3.6.4 Access Enforcement](#).
- All audit requirements pertinent to the Agency must be adhered to ([ISP 3.6.1 Audit Trail System](#)).
- Public-facing Internet applications must go through the [Authentication Risk Assessment \(ARA\)](#) in order to evaluate the risks of transactions within electronic applications, or services provided over the Web and automated telephone system.

**3.1.7.2 External Clients (Accessing SSA Web Services from outside of SSANet)**

- Externally facing Web Services require NIST-compliant authentication; the organizational credential would always be required for access to the Web Service. Exclusion to this policy allows for the elimination of server-to-server authentication if the Authentication Risk Assessment (ARA) determines that the Web Service is publicly consumable, and the Web Service client is part of a Commercial Off-the-Shelf (COTS) product designed for mass distribution. All other IT security controls apply

- Authentication for External Clients:

- Entity Authentication:

- (b) (7)(E) [Redacted]
- (b) (7)(E) [Redacted]
- (b) (7)(E) [Redacted]
- (b) (7)(E) [Redacted]

- (b) (7)(E) [Redacted]
  - (b) (7)(E) [Redacted]
  - (b) (7)(E) [Redacted]
- Individual Authentication:
    - (b) (7)(E) [Redacted]
    - (b) (7)(E) [Redacted]
    - (b) (7)(E) [Redacted]
- An agreement [e.g., Memorandum of Understanding / Agreement (MOU / MOA), Inter-Agency Agreement (IAA), Inter-connection Security Agreement (ISA), etc.] are required for a Web Service application when any of the following criteria apply:
    - SSA is disclosing data (e.g., records protected by the Privacy Act) to an outside entity;
    - The agreement is reimbursable;
    - The exchange is with another government agency; or
    - The ARA determines if a level 3 authentication is necessary – high business risk.

**NOTE**

*There may be other circumstances that require an agreement. Determinations must be made on a case-by-case basis in consultation with the Offices of General Law (OGL) and the Office of Privacy and Disclosure (OPD).*

### **3.1.8 Cloud Security**

#### **3.1.8.1 Background**

This subsection applies to all SSA components engaged in, or considering the outsourcing of, IT services to [Cloud Service Providers \(CSP\)](#), as well as any acquisition of cloud-based products and services from external CSPs.

#### **3.1.8.2 Procedure**

Organizations and components seeking external cloud-based services must first contact the CIO for approval. When considering external cloud-based products and services, it is SSA policy that no sensitive, Personally Identifiable Information (PII), or Federal Tax Information (FTI) is stored in, transmitted to, or processed in externally hosted CSPs without explicit authorization. Furthermore, the decision to authorize sensitive, PII, and FTI data in the cloud is based on proper [system categorization documentation](#) to be completed by the Security Authorization Manager

(SAM) or Component Security Officer (CSO), that must be submitted to the CISO for CIO consideration.

The use of external cloud-based products and services are subject to SSA's Security Assessment & Authorization ([SSA&A](#)) Policy. Cloud-based systems must comply with Federal Information Security Modernization Act [FISMA](#) requirements, Federal Risk and Authorization Management Program ([FedRAMP](#)) requirements, and any additional agency requirements contained within this ISP.

### **3.1.8.3 Cloud Deployment Model**

Cloud computing is defined to have several deployment models. For reference purposes, NIST defines the following cloud deployment models:

- **Private cloud** – The cloud infrastructure is provisioning for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may own, manage, and operate by the organization, a third party, or some combination of the two; it may exist on or off premises.
- **Community cloud** – The cloud infrastructure is provisioning for exclusive use by a specific community of consumers. These include organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may own, manage, and operated by one or more of the organizations in the community, a third party, or some combination thereof; it may exist on or off premises.
- **Public cloud** – The cloud infrastructure is provisioning for open use by the public. It may own, manage, and operate by a business, academic, or government organization, or some combination thereof. It exists on the premises of the cloud provider.
- **Hybrid cloud** – The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

### **3.1.8.4 FedRAMP Security Requirements**

Under the lead of the General Services Administration (GSA) and NIST, FedRAMP was developed to establish trust relationships between Federal agencies, and CSPs. Under FedRAMP, minimum security requirements are established for Federal cloud services.

All agency procurements of externally hosted cloud products and services must comply with FedRAMP security requirements.

- System categorization is required prior to FedRAMP security authorization initiatives. Sensitive data, like PII or FTI information, must be authorized to use in externally hosted CSP's by the CIO through the CISO's approval. This process must be considered by the designated authorization personnel upon receipt of system categorization documentation adhering to FIPS-199 standards from the Office of Information Security representative.

- Prior to deploying externally hosted cloud products and services, the CSP must conduct a security assessment using a FedRAMP-authorized Third-party Assessment Organization (3PAO) in order to meet FedRAMP provisional authorization requirements. The agency component seeking to procure external cloud services must coordinate with the Office of Acquisition and Grants (OAG) to ensure this requirement is included in the contract award or grant.
- SSA may request FedRAMP provisional authorization documentation from the FedRAMP PMO as evidence that minimum FedRAMP security controls have been effectively implemented by the external CSP and granting the provisional authorization.
- SSA must use the FedRAMP Provisional Authorization in conjunction with additional security assessment information when making Authority to Operate (ATO) decisions. Furthermore, the sponsoring component must also adhere to the agency SSA&A Policy Handbook and SSA Security Authorization Process for External Systems guide.
- The business sponsor must complete a Risk Assessment that considers the applicable threats and vulnerabilities, as well as the effectiveness of the Information System's safeguards and countermeasures. Furthermore, the sponsoring component must document acceptance of risk and obtain concurrence by the Designated Authorizing Authority (DAA) as outlined in the Risk Acceptance Handbook.

#### **3.1.8.5 Agency Security Requirements**

All cloud-based solutions, providers, and supporting infrastructure must be located in the United States, its territories, and possessions.

When considering external cloud-based solutions, components are encouraged to consider geographic dispersion and the threat of natural disasters in planning requirements for where agency information may be stored.

The use of external cloud-based products and services are subject to SSA's [SSA&A](#) Policy.

#### **3.1.8.6 Chief Information Officer Approval**

Components or Regions planning to leverage external cloud services must advise and maintain written approval of the DCS/CIO when planning an acquisition. CIO approval documents should be provided as part of any related or potential cloud service acquisition to the OAG. New SSA Cloud Systems shall be added to the official SSA Cloud Systems list maintained by Office of Systems Architecture (OSA), Division of Enterprise Architecture & Data Administration (DEADA) and reviewed at least annually.

Only the CIO can make the risk-based determination to use IT systems. The CIO can leverage the FedRAMP provisional authorization, including security authorization packages and all

supporting documentation, when making his or her own risk-based decision to grant ATO for external cloud services.

### **3.1.9 Mobile Device Security**

#### **3.1.9.1 Background**

SSA's Mobile Device Security policy applies to all agency issued mobile computing devices (e.g. laptops, tablets, cell phones, smart phones with data/network connectivity). Personally owned mobile computing devices are not authorized to connect to SSA's network.

All SSA mobile computing devices must be authorized ([See ISP section 2.1.2.](#))

Only authorized users are allowed to access SSA resources via approved agency mobile devices.

Mobile computing devices must be in compliance with the agency security standards document for the device:

- Downloading or installing unauthorized software onto agency devices is prohibited.
- Unauthorized altering of agency devices is prohibited.
- Unauthorized disabling of any software or hardware on SSA devices is prohibited.
- Devices must implement a screen lock and require an SSA approved method to unlock.

All mobile computing devices are required to have full device encryption that complies with current Federal standards.

#### **3.1.9.2 International Travel**

International travel is defined as travel conducted outside the continental United States, Alaska, and Hawaii. Individuals holding security clearances (b) (7)(E), (b) (2)

Some countries restrict the use of electronic devices, as well as encryption technology. If taking an agency-issued cell phone, mobile computing device, or media on official foreign travel, the traveler must contact a US Embassy or Consulate in the destination country for possible country specific information regarding prohibitions against electronic devices and / or encryption technology.

Agency issued cell phones and mobile computing devices may only be taken on international travel by SSA employees, Disability Determination Services (DDS) employees, temporary staff, contractors, and other users acting on behalf of the SSA. International travel with these devices are allowed only when there is a substantial business need as determined by the requestor's component; the Office of Information Security (OIS) has conducted a security review; and the

[international travel request form](#) has been approved by the agency Chief Information Security Officer (CISO).

***NOTE***

*An International Travel Request Form must be completed and submitted in advance of travel to allow adequate time for processing.*

Personnel must consider options in support of the business justification that pose the least amount of risk.

- Cell phones when voice-only capability must satisfy the users communication requirements.
- Smartphones when secure-messaging capability is required.
- Laptops when mobile-computing capability is required.

If an agency security configuration standards document does not exist for a mobile computing device, the device may not be taken on international travel. Operating system and application software must be fully patched and anti-malware software current. Cell phone / smartphone taken on international travel must be managed by the OSOHE.

Travelers may only use agency-managed / configured laptops to conduct official business during foreign travel. No portable media provided by non-agency personnel (e.g., foreign officials) shall be used on laptops or be connected to any agency computer, device, or system.

Travelers must not store SSA property in checked baggage or leave the property unattended in a non-secure location.

Travelers must report a lost, stolen, and / or compromised device to the National Network Service Center (NNSC) at 1-877-697-4889 to initiate an incident report procedures. The traveler must also report any equipment loss to the Control Officer or the Regional Security Officer at the US Embassy or Consulate. The OSOHE must immediately invoke a remote wipe command to disable the smartphone and suspend all phone services.

For personal safety, SSA personnel must comply with instructions from foreign officials and if necessary, follow procedures for reporting lost, stolen, or compromised devices as soon as feasible following an incident of loss.

## 3.2 Awareness and Training

The following subsections provide policy and guidance related to the agency's annual information security training requirements

### 3.2.1 Information Security Training and Awareness Policy

SSA mandates annual information security awareness training, role-based training for personnel performing roles with significant cybersecurity responsibilities, and the reporting and retaining of completed training.

Additional, as specified by FISMA and NIST information security training requirements, SSA conducts social engineering exercises on an ongoing basis.

SSA's Information Security Training and Awareness Program derives its requirements and direction from:

- [The Federal Information Security Modernization Act of 2014 \(FISMA\)](#).
- [National Institute of Standards and Technology's Special Publication 800-16](#), Information Technology Security Training Requirements: a Role- and Performance-based Model.

The following requirements must be met:

- All SSA information systems users must complete [Mandatory Information Security Awareness Training](#) within forty-five (45) days of onboarding.
- All SSA information systems users must complete [Mandatory Information Security Awareness Training](#) each Fiscal Year (October 1st to September 30th).

#### **NOTE**

*Any information systems user who does not complete refresher training by the end of the communicated training deadline may face adverse action.*

For additional information security awareness material, please visit the [Cybersecurity Communication & Training Portal](#).

For records retention, component management must follow the established SSA [record retention schedules](#) for all information security-related training records.

### 3.2.2 Role-Based Training for Personnel with Significant Cybersecurity Responsibilities

- **(b) (7)(E), (b) (2)**, all information systems users, including contractors, with significant cybersecurity responsibilities must complete role-based cybersecurity training, in addition to information security awareness training.



- Please visit the [Role-Based Cybersecurity Training Portal](#) for criteria the agency uses to identify personnel with significant cybersecurity responsibilities, specific employee and contractor training requirements, and available training resources.

### 3.2.3 Training Records Retention

The following requirements must be met:

- Component management must follow the established SSA record retention schedules for all information security-related training records.

### 3.2.4 Agency Reporting of Information Security Training

The following requirements must be met:

- For audit purposes, each component is responsible for providing, upon request, evidence of completed awareness and/or role-based cybersecurity training.
- Component management, along with Contractor Officer Representatives (COR), jointly submit evidence, upon request, of completed awareness and/or role-based cybersecurity training by contracted personnel.

## 3.3 Data Security

The policies in this section ensure information and records are managed consistent with the SSA's risk strategy to protect the confidentiality, integrity, and availability of information.

### 3.3.1 Protection of Information in Transit and at Rest

Project Managers (PMs) must consider encryption as part of their risk assessments, when developing systems using the agency's System Development Lifecycle (SDLC). Factors to consider include the information maintained or transmitted by the application, as well as the sensitivity level assigned. In order to ensure security of agency information, the agency requires the following:

- Encryption is required for sensitive or mission critical data, while at rest or in transit (See [ISP Section 2.1.3](#) for data categorization information)
- (b) (7)(E), (b) (2) critical data transmitted beyond the SSA Network (SSANet), (i.e., external to the firewall) must be encrypted or otherwise protected as approved by the Chief Information Security Officer (CISO).
- Authorized technical support personnel (i.e., (b) (7)(E), (b) (2) can use unencrypted, SSA approved, removable media that contains non-sensitive information for hardware and software administration and technical support activities.
- Files encrypted for external users require a minimum password length nine (9) characters.



- The password (also called a key) must include both a number and a special character.
- When delivering the password, do not include it in the same email as the data or ship it in the same package as the media.
- Encryption-related information (such as passwords) must be secured when unattended or not in use.
- It is prohibited to decrypt information a user is unauthorized to view.
- Use only agency-approved and managed encryption software.
  - Staff may use software that was included with agency-purchased devices.
  - Staff may not use personally owned encryption software.
- The encryption method employed must meet acceptable encryption standards designated by the National Institute of Standards & Technology (NIST).
  - The encryption method to secure data is the Advanced Encryption Standard (AES) with a minimum 128-bit cipher.
  - The encryption algorithms in use must conform to NIST's Cryptographic Module Validation Program as required by Federal Information Processing Standards (FIPS) 140-2, as amended. Please see [\(Cryptographic Module Validation Program \(CMVP\)\)](#) for more information.
- Those considering the use of other algorithms must submit a request for exception to the CISO in the Office of Information Security (OIS).

### **3.3.1.1 Laptop Encryption**

All laptops are required to have full disk encryption that complies with current [Federal Information Processing Standard \(FIPS\) Publication 140-2 requirements](#).

The Office of Systems (DCS) has procured solutions for the vast majority of laptops owned by the agency. Technical instructions for installing this software can be found at the (b) (7)(E) webpage.

### **3.3.1.2 Removable Media Encryption**

The DCS has procured a solution to encrypt media containing sensitive data that is transported or stored offsite. This includes, but is not limited to, USB flash drives, CDs, or DVDs containing sensitive information. For additional information and guidelines for using the McAfee File and Removable Media Protection (FRP) software, see [McAfee File and Removable Media Protection \(FRP\) SharePoint Site](#).

### 3.3.1.3 Key Management

The System Owner (SO) is responsible for determining the need for public keys (e.g., certificates), acquiring them and for the lifecycle management of keys utilized for their respective systems. For certificate-based public keys, the Office of Systems Operations and Hardware Engineering (OSOHE) serves as the SSA Registration Authority (RA).

### 3.3.2 Data Protection throughout the Lifecycle

#### 3.3.2.1 Data Custodianship

SSA data, and information derived from data, are vital business resources used in all of the offices and divisions throughout the agency. Often, data and information from one particular business area is relevant and applicable to other business areas, leading to data/information sharing. Data Custodianship is the principle of responsibility in the management and protection of data while in one's possession. Data Custodians have administrative and/or operational responsibility over SSA data and information. Any individual accessing SSA data is considered to be in possession of that data. Responsibilities of a Data Custodian apply to data in their possession, regardless of how the data is obtained, and include:

- Manage access to and processing of data in accordance with principles of least privilege, need-to-know, and other policies and procedures outlined in ISP Section 3.1, Access Control.
- Ensure data is used for the authorized purpose and protect data from unauthorized use.
- Understand, monitor, and document how data is stored, processed, and transmitted.
- Assess level of sensitivity, if not explicitly defined, based on potential impact a loss of the data would have on organizational operations, assets, or individuals.
- Protect and store data in manners appropriate for the level of sensitivity.
- Verify compliance with relevant legislation, including privacy, for data release.
- Disclose and follow-up on reports of data access violations.
- Adhere to change management practices.
- Assure data content and changes can be audited.
- Abide by and enforce data retention and disposal policies.
- Transport data according to agency policies.

Data management must uphold the security objectives of confidentiality, integrity, and availability throughout the data lifecycle, through security controls and adherence to the following security principles:

- **Provisioning** - Enforce principles of least privilege, need-to-know, and separation of duties as defined within [ISP Section 3.1, Access Control](#).
- **Access** - Manage access to data in accordance with policies and procedures discussed within [ISP Section 3.1, Access Control](#).
- **Usage** - Use data for intended purpose with a specified start and end timeframe.

- **Protection** - Defend data from unauthorized view, use, modification, and disposal.
- **Storage** - Store data in a manner appropriate for its classification and maintain physical control of the data.
- **Transport / Exchange** - Transport or exchange data in accordance with agency policies.
- **Retention and Disposal** - Enforce data retention and disposal policies.

### 3.3.2.2 *Removable Media*

The local Manager is responsible for enforcing the following policies:

- Ensure that mobile computing devices are secure when not in use (e.g., hand-held PCs, Smartphones, USB flash drives, etc.).
- Ensure that all critical information and applications residing on LAN servers are backed-up regularly.

### 3.3.2.3 *Handling and Exchange*

In adherence to the security principles of least privilege, separations of duties, and need-to-know, the handling and exchange of data include the following:

- **Request** - Obtain data in accordance with required processes related to the data source.
- **Approval** - The approver reviews the request for the business need and approves or denies it.
- **Authorization** - A subject matter expert (SME) familiar with the data type(s) requested must review all requests to affirm validity of the request. If satisfactory, the SME will grant appropriate access to the data.
- **Review** – (b) (7)(E), assess whether continued business need for access to data exists. If access is no longer needed, disable access to, and/or discard data.

### 3.3.2.4 *Definitions*

- **Data** - Facts or figures to be processed, evidence, records, statistics, and/or any other type of information that can be analyzed and/or interpreted by a human or a machine.
- **Information** - Result of data processed, organized, structured, or presented in a given context.
- **Sensitive Information** - Information protected from unauthorized disclosure. Includes, but is not limited to, Personally Identifiable Information (PII), Federal Taxpayer Information (FTI), Protected Health Information (PHI), Controlled Unclassified Information (CUI), Payment Card Industry – Data Security Standard (PCI-DSS), and SSA proprietary business data.
  - **Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number,

- date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. See [NIST SP 800-122](#).
- Federal Taxpayer Information (FTI) - Any return or return information received from the IRS or secondary source, and includes any information created by the recipient derived from the return or return information. An example of FTI is data found within the Master Earnings File (MEF). See [IRS Publication 1075](#).
  - Protected Health Information (PHI) – All individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. See the [HIPAA Privacy Rule](#).
  - Controlled Unclassified Information (CUI) – Information the Government creates or possesses, or that an external entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. See the [CUI Policy](#).
  - Payment Card Industry – Data Security Standard (PCI-DSS) – A set of standards that helps to protect cardholder data. It applies to all entities that store, process, or transmit cardholder or sensitive authentication information. See the [PCI Security Standards Council](#).
  - Proprietary Business Data - Material and information relating to, or associated with, SSA products and services, business, or activities. These include, but are not limited to, SSA administrative data. Major sources of SSA administrative data are, but are not limited to, the following records systems:
    - Master Beneficiary Record (MBR) - Payment file from which Social Security checks are paid. The MBR contains information on Title II beneficiaries, such as payment status, type, and amount.
    - Supplemental Security Record (SSR) - Payment file from which Social Security Income (SSI) checks are paid. The SSR contains information on Title XVI beneficiaries, such as payment status, type, and amount.
    - NUMIDENT - Master file of assigned Social Security Numbers (SSNs). This file contains identifying information given by the applicant for an SSN.
    - Master Earnings File (MEF) - File of workers' earning records and information on the individual's entire work experience.
    - Death Master File (DMF) - Publically available database containing death notices for individuals enrolled in the U.S. Social Security program since 1936.
    - Document Management Architecture (DMA) - Architecture that addresses SSA document capture, indexing, routing, storage retrieval, and management needs. DMA uses hardware and software components to create an object repository for storage and retrieval of information.

### 3.3.3 Data Integrity

#### 3.3.3.1 Automated Integrity Reviews

Automated integrity review controls must be considered as compensating controls to address inherent business processes that result in risks for improper payment, improper disclosure, fraud, and abuse of sensitive agency information. Compensating controls are required to mitigate any lack of operational separation of duties. OIS works in conjunction with the user community to develop integrity review requirements. For further discussion on the integrity review process refer to the Integrity Review Handbook (IRH).

#### 3.3.4 IT Equipment Safeguards

The U.S. Government restricts the export of encryption technologies. Residents of countries other than the U.S. should also make themselves aware of the encryption technology laws of the country in which they reside.

The statutory authority for the SSA records management program is the [Federal Records Act of 1950](#), as amended (Title 44, United States Code (USC), sections 3101-3107 and 3301-3314, which outlines the requirements for proper disposal of privacy related information. The [Federal Records Act](#) requires each Federal agency to establish and maintain an active, continuing program for the economical and efficient management of its records. These instructions generally pertain to files, folders, and formal records, as well as cover transfer, and recall to and from the Federal Records Center.

#### 3.3.5 Secure Email Use Policy

Email is considered unsecure unless there are special steps taken to protect it. For example, anyone with appropriate privileges to the email servers used to send an email can access and read it. Therefore, employees must consider whether the information contained in an email needs to be protected from improper disclosure and use the following agency procedures to send it securely:

- Email is an official business communication tool and users must use it in a responsible, secure, and lawful manner.
- Only send email containing Personally Identifiable Information (PII) or other sensitive information to email addresses that are secure ([secure partners list](#)). Advise any individuals and agency contacts to not send SSA their personal information via unsecure email.

If SSA employees, vendors, contractors, grantees, or agents operating on behalf of SSA receive an email message intended for someone else, immediately notify the sender and delete or destroy the misdirected message.

Individuals using SSA email must comply with all requirements specified in the Policy On Limited Use of Government Office Equipment Including Information Technology. ([Agency Use of Government Equipment](#)).

Internal email sent within SSA’s network (name@ssa.gov) is secure. Email that leaves SSA is secure if it is to an organization listed in the (b) (7)(E)

The following table illustrates when information is sent securely and insecurely via email and therefore must be protected by encryption.

Sent from	Received by	Result	PII Allowed in Message
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)

**NOTE**

*ALL email recipients (To, Copy (cc), and Blind Copy (bcc) address fields) must be secure for the message to be considered secure. The presence of one non-secure addressee renders the entire message Not Secure.*

*Remember, you can have a PII breach or unauthorized disclosure by sending a secure email to a person not authorized to have that information.*

Special rules apply to e-mail messages containing PII that SSA sends to the (b) (7)(E), (b) (2)

[Redacted]

(b) (7)(E), (b) (2)

When emailing protected information to a non-secure recipient by sending it within an encrypted attachment, you must provide the password separately (e.g., by phone or in person). If contact by phone or in person is not possible, you may send the password in a separate email message either before or after transmitting the message with the encrypted file(s). You must never send the password in the same email containing the encrypted attachment that the password protects. Do not use an SSN or an individual's name as the name of the encrypted attachment.

**NOTE**

See [Encryption Methods](#) for approved encryption options.

Do not send or forward information that requires confidentiality or protection from disclosure to non-SSA accredited mobile devices. Examples of mobile devices include, but are not limited to:

- Personal Data Assistants (PDAs)
- Two-way pagers
- Smartphones (i.e., iPhone, Android phone)
- Cellular telephones
- Tablets, Laptops and other personal computing devices

Do not send or forward PII (or other information that requires confidentiality or protection from disclosure) using a non-SSA (or non-secure) email account to anyone. Examples of non-SSA email accounts include, but are not limited:

- Gmail
- Hotmail
- Yahoo mail
- AOL mail
- Any email provided by Internet Service Providers

Non-secure example: An agency employee working at home uses their personal e-mail account to transmit work related PII to their work address or a third party.

Do not send or forward PII (or other information that requires confidentiality or protection from disclosure) to a non-SSA email, account unless the recipient is listed as secure or the information is protected by an encrypted attachment. For a non-secure example: An agency employee forwards an agency email containing PII to a lawyer's office assistant, whose email is not secure.

Do not send email to Federal agencies, including Congressional offices, with PII in the subject line, the body of the email, or in any unencrypted attachments to the message, unless recipient is listed as a secure partner above.

Do not configure an SSA email account to automatically forward work related email to an outside (non-SSA, non-secure) address. For a non-secure example: An agency employee sets up an Outlook rule to send a copy of all work related emails to a personal email account so as to be able to work outside the office.

Do not copy (i.e., cc, or bcc) work related email to your personal non-SSA e-mail account. For a non-secure example: An employee concerned about a performance appraisal bcc's correspondence between her supervisor and herself, much of which contains claims specific information (PII), to her personal non-SSA email account.

Do not include sensitive or protected information in an email reply unless the recipient has secure email or an encrypted attachment protects the information. Pay particular attention to not re-expose PII in your response when your reply includes incoming or prior emails that contain PII (contained in those messages).

**NOTE:**

*Users who fail to adequately protect sensitive information or agency resources, or who violate agency security policies, may be subject to disciplinary action up to and including termination or other actions in accordance with applicable law and agency policy.*

### **3.3.6 Secure Fax Use Policy**

A Fax is an official business communication tool and users must use it in a responsible, secure, and lawful manner.

When sending citizen, programmatic, or other protected information externally via Fax, use a Fax cover sheet that includes a notation that the material contains sensitive information and only delivering to the addressee.

Users must ensure that documents transmitted via Fax go to the intended person(s) and when practical, use preprogrammed Fax numbers to ensure correct routing.

Do not leave fax machines unattended during transmission of citizen, programmatic, or other protected information.

If SSA employees, vendors, contractors, grantees or agents operating on behalf of SSA receive a Fax message intended for someone else, immediately notify the sender and delete or destroy the misdirected message.

Individuals using SSA fax systems must comply with all requirements specified in the Policy On Limited Use of Government Office Equipment Including Information Technology. ([Agency Use of Government Equipment](#)).



### **3.3.7 Prohibited Security Practices / Activities**

Individuals who have rights / privileges to view others' e-mail/Faxes are prohibited from doing so unless authorized by appropriate management officials. See <http://aims.ssahost.ba.ssa.gov/GAM/G1416.htm> for policy governing how to access an employee's workstation.

### **3.3.8 IRS Federal Tax Information (FTI)**

The agency handles and maintains FTI in many of its business processes. Therefore, the audience for this section is agency component Managers, Information Security Officers, employees, and contractors. The section provides four (4) important pieces of information. First, it provides policy on protecting FTI from unauthorized usage and improper disclosure. Second, it describes what defines FTI. Third, it describes sanctions applicable to employees, and contractors that misuse FTI. Finally, the section provides procedures to follow when unauthorized access to FTI, or improper disclosure of the information occurs.

#### **3.3.8.1 Directive**

The IRS has authorized the agency to handle and store FTI as part of its business processes. IRS Code (IRC) 6103 is a confidentiality statute and generally prohibits the disclosure and usage of FTI for unauthorized reasons. Agency policy is to use FTI solely for the purposes authorized by IRS. Moreover, it is agency policy to protect the confidentiality of FTI from unauthorized usage and improper disclosure and, to the extent that it is practical do so, meet the requirements of IRC 6103.

#### **3.3.8.2 What is FTI?**

Generally, FTI includes any return (or information transcribed from it) required to be filed under the IRC. Important, if the source of data was IRS, via an electronic data exchange, or return information processed by SSA on behalf of IRS, the information is FTI. The key determinant of FTI is its source. For a more extensive description of FTI, see IRS Publication 1075. Following are some examples of FTI.

An individual's annual earnings (wages) and net earnings from self-employment in SSA's records constitute FTI because the information is gathered from an IRS-SSA electronic data exchange. However, individual address information may or may not be FTI depending on its source. For instance, if the information from a W-2 or other return, it is FTI. However, if the information was obtained directly from an SSA beneficiary, it is not FTI—same data element, but two different sources.

### **Sanctions and Unauthorized Inspection — Important Reminders to All Employees and Contractors to SSA**

IRC Section 7213 prescribes criminal penalties for Federal and state employees and others who make illegal disclosures of FTI, which is a felony offense. Additionally, IRC Section 7213A makes the unauthorized inspection of FTI a misdemeanor punishable by fines, imprisonment, or

both. IRC Section 7431 prescribes civil damages for unauthorized inspection or disclosure and upon conviction, the notification to the taxpayer that an unauthorized inspection or disclosure of FTI has occurred. For additional information, see [IRS Publication 1075](#)

### **3.3.9 Disclosure Policy**

In accordance with disclosure and privacy law and rules, agency information, including PII can only be shared, released or disclosed to persons or organizations authorized to receive it. Additionally, disclosure requirements apply to other kinds of information that also must be kept confidential ([GN 033 Disclosure / Confidentiality of Information, the Office of Privacy and Disclosure website](#), [AIMS, GAM 14.09](#), or contact OPD at [OGC OPD Controls](#)).

Disclosure of information is only allowed for authorized purposes or otherwise as permitted by law. Any information (including PII) about an individual in electronic form (such as email or Fax) must be protected to the extent that a paper record is protected under the Privacy Act of 1974.

Protected citizen and programmatic information may be transmitted via email for official business purposes only ([Office of General Counsel/Office of Privacy and Disclosure](#)).

### **3.3.10 Records Retention Policy**

SSA personnel are responsible for retaining or destroying electronic records in compliance with SSA policy located at the Office of Publications and Logistics Management (OPLM), Office of Document Management (ODM), Records Management (RM) Intranet site.

Additional information on records retention is located on the [Records Management](#) website.

### **3.3.11 Mandatory Encryption of Electronic Data on Mobile Computers and Devices**

SSA's implementation of OMB directives for protecting PII using encryption (including email) is found in the Administrative Instructions Manual System, [General Administration Manual, Chapter 15.04.04](#).

### **3.3.12 Other Agency Guidance on Email/Fax Not Listed Above**

The DCS has prepared a document on [Email Guidelines](#) and has information on [Internet email online](#), as well.

Email security and Fax best practices are in the [PII FAQ](#).

### **3.3.13 Paper Records Disposal**

Individual offices / components may accomplish proper paper records disposal by designating separate burn bags or shredding individual documents. IRS tax information must be shredded to the specifications previously agreed by the IRS (see IRS Publication 1075, Chapter 8.3).

Sensitive material must be definitively destroyed in accordance with the instructions in [SSA AIMS Material Resource Manual \(MRM\), Records Management Handbook Chapter 4](#). These instructions generally pertain to files, folders, and formal records, as well as cover transfer, and recall to and from the Federal Records Center.

### 3.4 Information Protection Process Policy

This section encompasses policies used to manage protection of information systems and assets.

#### 3.4.1 Configuration Management

Configuration management standards are the first line of defense for the prevention of malicious activities on SSA networks. All system owners must document detailed baseline configurations for information systems. These baseline configurations must be maintained throughout the system lifecycle.

Baseline configurations and inventories of information systems (including hardware, software, firmware, and documentation) must be established and maintained throughout the respective system life cycles, and security configuration settings for information products employed in information systems must be established and enforced.

- Scanning and monitoring of system configurations will be performed on a regular basis. System owners will be notified and are expected to correct any deviations discovered.
- All hardware, software, and platforms must have security configuration guidelines and standards so that they can be configured properly to ensure effective security.
- Operating Systems and application software must be fully patched and anti-malware software current.

The following prohibitions apply to all SSA hardware, software, and associated platforms:

- Downloading or installing unauthorized software onto agency devices;
- Connecting unauthorized hardware or personal devices to SSA's IT infrastructure; the IT infrastructure includes, but is not limited, to workstations, servers, routers, switches, and cable connectors, as well as wired and wireless network resources;
- Unauthorized alteration of agency devices;
- Unauthorized use or copying of SSA software; and
- Unauthorized disabling of any software or hardware on SSA devices.

**NOTE:**

*Users who fail to adequately protect sensitive information or agency resources, or who violate agency security policies, may be subject to disciplinary action up to and including termination or other actions in accordance with applicable law and agency policy.*

### 3.4.1.1 Security Configuration Standards

[Authorized platforms](#) and [solution architectures](#) are required to have an authorized security configuration standard. [Security configuration standards](#) must be reviewed annually.

All platforms must follow the subsequent web security standards:

- All agency Internet and Intranet websites and services must deploy Hypertext Transfer Protocol Secure (HTTPS) and enable HTTP Strict Transport Security (HSTS).
- All agency public-facing websites and services must be configured with HTTPS only, HSTS, and a strong certificate with a publicly verifiable chain of trust, as documented on the [External Websites Certificates](#) site.

Internet facing (b) (7)(E) platforms must be configured as follows:

- (b) (7)(E)
- (b) (7)(E)

### 3.4.1.2 Exceptions

Agency components may seek approval to deviate from standard SSA baselines, security configuration settings, or guidelines for desktop software, a specific platform (e.g., Windows, UNIX), and for wireless or off-net Internet connections by submitting a [Request for Exception](#). The Office of Information Security (OIS) must approve or deny the exception request and notify the component of the final decision.

## 3.4.2 System Development Lifecycle Security

There are three (3) important aspects of computer security in relation to the SDLC:

1. Security must be considered from the first to the last phase of the system's life cycle.
2. Development of computer security is an iterative process. The identification of vulnerabilities, and potential threats, and the selection and implementation of safeguards continue as the system progresses through the phases of the life cycle, including after the system has been released into production.
3. All computer security considerations should be documented in the standard SDLC documents.

By making security an integral part of the SDLC, it ensures the security implications of new systems functionality, or changing agency conditions, are resolved in a systematic way.

Identifying vulnerabilities and developing safeguards increases awareness of security concerns by involving all components responsible for the development of the application in the process.

Proper implementation of this standard ensures SSA's compliance with Federal regulations. By embedding system security control architecture into the SDLC, SSA's software products conform to requirements, standards, and Federal guidelines as defined in OMB A-130, Appendix III and NIST SP 800-64, "Security Considerations in the System Development Life Cycle".

All security considerations should be documented in the standard SDLC documents. To properly manage risk during development and maintenance of SSA software products, organizations and components must incorporate the Information Security components of the SDLC. SDLC risk management encompasses the following elements:

- Categorize the System and Select Security controls.
- Document, Implement, and Assess Security Controls.
- Authorize the Information System.
- Monitor Security Controls.
- Ensure orderly termination of the system.
- System categorization and asset identification,
- Initial security risk assessment,
- Security requirements development,
- Security planning and control development,
- Security control integration,
- Final security risk assessment,
- Security Assessment & Authorization (SA&A),
- Configuration and change control
- Continuous monitoring and risk assessment updates.

#### **3.4.2.1 Information Technology (IT) Contract Requirements**

Information Technology (IT) includes any system that collects, processes, transmits, stores, or disseminates agency information. For contracting information and regulations, see the [Office of Acquisitions and Grants](#) (OAG) website. For agency specific security-related clauses, see OAG's [Contracting Officer's Technical Representatives \(COTR\) Resources](#) webpage.

All personnel involved with the contracting and grant processes must integrate necessary security requirements into all phases of the acquisition cycle. These include planning, solicitation, review of offeror's proposals or quotes, contract award, and contract administration. As used in this section, the term "contract" includes, but is not limited to, contracts, contract modifications, purchase orders, delivery orders, task orders, and grants.

Every solicitation or contract involving IT, or affiliated SSA IT resources, must include appropriate security requirements. Information Security clauses for IT must comply with security requirements prescribed by the National Institute of Standards and Technology (NIST) under

authority of the Federal Information Security Modernization Act (FISMA). Security requirements for inclusion in SSA solicitations are provided in *Information Security for Acquisitions*.

To ensure proper handling of sensitive information, the contractor must submit a Systems Security Plan (SSP), as applicable, before SSA transmits sensitive information to the contractor.

Additionally, the contractor must continuously monitor the status of implemented security controls to ensure their continued effectiveness.

### 3.4.3 Web Application Development Policy

#### 3.4.3.1 Web Application Development Rules

The term application includes, but is not limited to, frameworks, services, source code, and other software. This policy applies to all SSA personnel, contractors, temporary staff, and any other users when acting on behalf of SSA to develop all Internet and Intranet web applications.

The following requirements apply to all Internet applications:

- An agency approved code analysis tool must be used to evaluate source code.

**NOTE**

*Based on code analysis results, OIS may determine that an application requires penetration testing. (See the [Penetration Test Site](#).)*

- All applications must have a maximum time-out feature of 30 minutes.
- The following web measurement and customization technologies (e.g. cookies) may be used:
  - Tier 1 (Single Session)
  - (b) (7)(E)

**NOTE**

(b) (7)(E)

- All publicly accessible websites must be fully compliant with [SSA's Internet Privacy Policy](#).

The following requirements apply to all **Intranet** applications:

- An agency approved code analysis tool must be used to evaluate source code for the following types of applications:
  - (b) (7)(E)

- (b) (7)(E) [REDACTED]
- Web measurement and customization technologies (e.g., cookies) are allowed (subject to the restrictions stated below).
  - (b) (7)(E) [REDACTED]
  - (b) (7)(E) [REDACTED]
  - (b) (7)(E) [REDACTED]
  - (b) (7)(E) [REDACTED]

The following requirements apply to both **Internet and Intranet** applications:

- Best coding practices must be followed as stipulated in the National Institute of Standards and Technologies (NIST) Special Publication 800-53, Open Web Application Security Project (OWASP) and Common Weakness Enumeration (CWE). This includes, but is not limited to:
  - Validate inputs and uploads
  - Manage authentication and authorization
  - Identify and handle error conditions
- All application code must be stored in an Agency-approved source code platform.

For additional development guidance, please see the [Web Application Security](#) webpage.

**NOTE**

*For guidance on Internet usage please see [SSA's Personal Use of Government Equipment](#) policy.*

### 3.4.4 Configuration Change Control

All information system configuration changes must be planned and implemented in accordance with the (b) (7)(E) process.

### 3.4.5 System Backup

System owners must develop a backup plan for all critical applications and assets that includes:

- Securing a backup storage facility (onsite and offsite);



- Ensuring that contracts for any offsite storage facilities follow all security policies for safeguarding and protecting Agency assets; and
- Testing backup plan procedures (b) (7)(E) to ensure that information is retrievable and available.

The above requirements are consistent with Department of Homeland Security (DHS) Presidential Directive HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection. The resulting plans are an important component of SSA's COOP, which is developed in compliance with the HSPD-6, Enduring, Constitutional Government and Continuity of Government Operations, OMB Circular A -130, and FISMA.

Contingency planning for SSA's Information Systems is a part of the agency's [Critical Infrastructure Protection \(CIP\)](#) process. As such, many of the steps required for contingency planning complete a part of developing and updating the agency's [COOP](#). The following considerations address specific IT assets and their relationship to the larger [COOP](#) process.

### 3.4.6 Media Sanitization

Prior to releasing to vendors, disposing, or donating IT equipment such as disk drives, magnetic tapes, floppies, CDs, DVDs, USB flash drives, the media must be sanitized or destroyed in a manner that prevents unauthorized disclosure of sensitive information. To sanitize IT media, use one of the following methods: Approved overwrite utilities, Degaussing, or Physical destruction of the media. See the [Media Destruction Table](#) for acceptable manners of physical destruction. For additional media disposal procedures, see the [Tape and Hard Drive Disposal Procedures](#).

The following applies:

- Reformatting the media does not overwrite the data. Since the data can be retrieved, reformatting is not considered acceptable for data destruction.
- Degaussing is an authorized sanitization methodology for magnetic media such as disk drives, tapes, and floppies.
  - Degaussing must be performed with a certified tool designed for the media being degaussed.
  - Certification of the tool is required to ensure the magnetic flux applied to the media is strong enough to render the information irretrievable.

#### **NOTE**

*Hard drives that are degaussed are no longer usable.*

- Physical destruction is used when degaussing or over-writing cannot be accomplished (for example, CDs, floppies, DVDs, damaged tapes, hard drives, damaged USB flash drive). Physical destruction of media must follow standards set by NIST (SP) 800-88 R1.



- In cases where PCs, hard drives, or other storage devices are sent offsite for repair and their information must be retrievable, the repair contract must include a requirement for non-disclosure by the servicing vendor.
- For information regarding the procedure for the donation and disposal of IT equipment, see SSA's [Personal Property Management Handbook](#).

### 3.4.7 Continuous Monitoring

The SA&A and RMF processes have been established to support the continuous monitoring and improvement of protection processes.

The POA&M is a process for communicating security weaknesses discovered during assessment activities along with the planned corrective actions and timeframes. POA&Ms assist the agency in assessing, prioritizing, and monitoring the progress of remediation efforts for Information Security weaknesses found in programs and systems.

The CIO, OIS, the OIG, SAMs, and other appropriate agency stakeholders use POA&Ms to track the progress of corrective actions. Progress toward meeting milestones is regularly evaluated throughout the remediation process, and may be revised with the CISO's approval to maintain reasonable and effective corrective action plans. This method allows milestones to be tracked and reassessed during the remediation process.

The SO or program official is responsible for notifying the CISO from the OIS, of any audit or evaluation of their program or system which resulted in the identification of Information Security weaknesses. Notification is accomplished by sending an email to (b) (7)(E), (b) (2). The OIS staff must review and work with the SAM, or their designee, to develop a POA&M based upon the overall level of Information Security risk posed.

The Cyber Security Assessment and Management (CSAM) tool is the agency-wide authoritative source for tracking Information Security weaknesses, including critical infrastructure vulnerability assessments and security control assessments. CSAM is maintained and administered by the Office of Information Security (OIS), and additional information about CSAM is contained in the [CSAM Single Sign-On Instructions](#) and [CSAM Users Guide](#). The Agency Audit Management System (AAMS) maintained by the DCBFQM, is the management tool for documenting and tracking all IG audits, including physical security, and other external audits.

SAMs or delegated program official must report at least quarterly on remediation progress by updating POA&M status in CSAM. Appropriate OIG personnel will be provided read-only access to POA&M information in CSAM. Information on POA&M update in CSAM is contained in the [POA&M handbook](#).

Once a POA&M has been fully remediated, the SAM or delegated program official must submit a closure request to OIS with appropriate supporting documentation. OIS must review the evidence provided and either approve or deny the request. If the closure request is denied, OIS must provide the rationale and / or indicate additional evidence needed to approve the request.

### 3.4.8 Incident Response

SSA's Information Security Program requires an ongoing agency process to monitor, detect, eliminate, mitigate, and report significant Information Security incidents and risks of physical and cyber-attacks on SSA's network infrastructure and to protect our systems and information.

This includes risks and incidents related to both information and Information Systems. The agency must:

- Comply with the Federal government-wide standard for reporting cyber security incidents to the United States Computer Emergency Readiness Team (US-CERT) (formerly FedCERT).
- Have an incident response process for responding to significant attacks with the goal of isolating and minimizing damage. The incident response process must:
  - Include Information Security incident reporting capability.
  - Enable sharing of information with other organizations, consistent with NIST guidelines.
  - Assist the agency in pursuing appropriate legal action, consistent with Department of Justice (DOJ) guidance.
- Provide timely technical assistance to agency Information System operators to include guidance for:
  - Detecting and handling Information Security incidents.
  - Compiling, and analyzing information regarding incidents that threaten agency assets.
  - Notifying Information System operators of current and potential Information Security threats and vulnerabilities.
- Conduct periodic testing to ensure that incident response plans are reasonable and effective and that incident response personnel understand their roles

The SSASRT, which provides incident reports to key management personnel including the Deputy Commissioner for Systems (DCS)/ CIO and the CISO is tasked with responding to incidents involving SSA computer systems. The team is also responsible for reporting major incidents to US-CERT as soon as a determination that a major incident is occurring.

The SSASRT is comprised of security staff (including the CISO), systems personnel, and OIG representatives. These individuals are technical consultants for their area of expertise. The SSASRT, receives reports of suspected incidents, responds to incidents involving SSA computer systems, and takes appropriate action. SSASRT reports major incidents to the DCS / CIO, the CISO, and other key personnel having incident-related management responsibilities and to the [US-CERT](#) as soon as it determines that a major incident is occurring. US-CERT's role provides a central focal point for incident reporting, handling, prevention, and recognition to ensure that

the government has critical services available in order to withstand or quickly recover from attacks against its information resources. US-CERT has the following primary purposes:

- Provide the means for Federal agencies to work together to handle security incidents.
- Share related information.
- Solve common security problems and collaborate with Information Analysis Infrastructure Protection (IAIP) to plan future infrastructure protection strategies, and deal with criminal activities that pose a threat to the critical information infrastructure.

### **3.4.9 Personnel Screening**

SSA's Information Systems security policy for SSA's Personnel Security and Suitability Program for IS-related positions is part of the overall Agency Information Systems Security Program. SSA's Personnel Security and Suitability Program policy complies with the Federal Government's [OMB Circular A-130, Appendix III](#), [OMB Circular A-123 Management's Responsibility for Internal Control](#), which requires all Federal agencies to implement and maintain a program that ensures adequate security for all agency information collected, processed, transmitted, stored, or disseminated in [general support systems and major applications](#).

Suitability background investigative screening is required for all Federal appointees, employees, and persons performing contract, voluntary, or indirect services for the Federal Government. This screening is in addition to the SSA Systems Security technical, operational, and management controls, and varies by situation.

Suitability determination is the responsibility of the Center for Personnel Security (CPS) (Deputy Commissioner for Human Resources (DCHR) / Office of Personnel (OPE) / CPS). Appropriate suitability investigations are required for new employees, appointees, special-program personnel, and on-duty employees who are promoted or reassigned into Public Trust or National Security positions of a higher risk / sensitivity level.

In addition, the implementation of [Homeland Security Presidential Directive 12 \(HSPD-12\)](#) requires that, effective October 27, 2005, an FBI National Criminal History Check (FBI fingerprint check) be completed and adjudicated before allowing a new hire to enter on duty and before allowing a contractor to begin work on a contract.

#### **Determining Proper Risk Levels**

SSA's Personnel Security and Suitability Program for Information Technology (IT) positions uses position sensitivity / risk levels. All SSA positions have designated levels commensurate to their public trust or national security responsibilities and their position's attributes as they relate to service efficiency.

Sensitivity / risk levels rank in accordance with the degree of potential adverse impact that an unsuitable person could cause to service efficiency. Suitability refers to whether the conduct of

an individual will interfere with, prevent effective performance in his / her position, or prevent effective performance of the employing agency's duties and responsibilities.

To ensure proper investigation type and timing, position risk-level designations properly establish an initial step in filling all SSA and contractor positions. The required investigation serves as a basis for ensuring that each individual employed in a sensitive or public trust position has the appropriate clearance for the position.

Documentation of the rationale underlying a final risk designation decision is retained for audit purposes. At SSA, the documentation resides in the [Office of Human Resources](#) system of personnel records. Contact the Office of Personnel's (OPE) [Center for Suitability and Personnel Security \(CSPS\)](#) with questions related to determining position risk designations.

### **Background Investigations**

Background investigations are required for the following positions:

- Appropriate background investigations for all SSA appointees start on the day of or before appointment to Federal service, as part of the entrance on duty process. Investigations for contractors, volunteers, and / or special program personnel start prior to the assignment and / or access to SSA systems, information, and facilities.
- Employees selected for, or moving to, a position that is at a higher risk levels than that which they previously occupied must meet the investigative requirements of the new risk level; an additional investigation may be required.
- Employees selected for, or moving to, a position that is at a higher risk / sensitivity level than previously occupied must complete paperwork for investigation for the higher-level position. He/she must also be re-fingerprinted.

### **Sensitive Position Changes**

Employees being reassigned or separating from SSA who occupy moderate / high risk or national security position or are moving from one sensitive position to another, often have keys to restricted areas, know passwords for systems entry, have manuals that contain information on sensitive operations, etc.

- Each component must ensure that identification passes and sensitive materials are returned, passwords are changed or deleted, login / PIN codes are deactivated or rendered useless for gaining further systems access, and in critical situations, locks on doors to restricted areas are changed, keys returned, etc.
- The CSO, CDSI, the Processing Center Security Specialist (PCSS) / Security Officer, or the Data Operations Center personnel responsible for systems security must certify and retain the completed checklist.

At the time an employee receives notice that management is proposing his / her removal, management can consider temporarily placing the employee in a lower risk position pending the

outcome of the proposed removal. When an employee resigns, a review of the employee's work from the past several months is completed. The checklist is also completed for all persons in this category.

## **Dealing with Adverse Reports**

When investigative reports reflect significant adverse and / or derogatory information, OPE, [CSPSM](#) may contact the subject and offer him / her opportunity to refute or explain derogatory information. This policy implements the principle of “due process” and prevents possible errors based on mistaken identity, unfounded allegations, or unknown mitigating circumstances. [CSPSM](#) must appropriately safeguard OPM’s and other investigative reports. They must disseminate them only in response to requests made through, and authorized by OPM under provisions of the [Privacy Act of 1974](#) and the [FOIA](#).

Contractor suitability is valid with the following restrictions:

- Cannot exceed the length of the contract.
- If a contract employee stops working on a contract, a new background investigation must be initiated
- If it has been a year or longer since the individual performed on a contract for which he / she was formally adjudicated, a new background investigation must be initiated.

## **3.5 Maintenance**

### **3.5.1 Controlled Maintenance**

The respective System Owner (SO), or entity, is responsible for maintaining the agency’s enterprise hardware and software. The maintenance and repair of all SSA systems must be performed and logged in a timely manner, with approved and controlled tools.

For more information regarding enterprise maintenance for hardware and software at SSA, please visit the [OSOHE Onestop Portal](#).

### **3.5.2 Remote Maintenance**

Remote maintenance of SSA systems must be approved, logged, and performed in a manner that prevents unauthorized access.

## **3.6 Protective Technology**

### **3.6.1 Audit Trail Systems**

ATS is one of SSA’s official repositories for audit trail data. Authorized users may access resources pertaining to the ATS at the [ATS SharePoint site](#). This site includes the ATS User Guide and detailed information about the composition of SSA’s audit records. CSOs can provide information about access to this resource for authorized users.

SSA's implementation of internal controls include audit trail systems and integrity review processes, along with additional Information System audit coverage areas (System and Application). Internal control requirements are designed to protect sensitive and non-sensitive information electronically stored on or transmitted by SSA's Information Systems. Policy requirements call for implementation of effective technical, operational and management controls to protect confidentiality, ensure integrity, and maintain availability of SSA data and information systems. Moreover, the policy requirements and guidelines provided in this subsection are intended to facilitate investigation in circumstances of potential improper payment, improper disclosure, fraud, and abuse.

The Audit Plan should be completed in conjunction with required FISMA documentation during the applicable stage outlined in the (b) (7)(E) process.

These requirements and guidelines apply to:

- New systems / applications (including Internet, intranet, client / server, non-Internet / Intranet application systems, standard development, and others).
- Modifications / Major changes to existing systems / applications.
- Systems / applications used within any part of SSA.
- Systems / applications developed in any SSA component (with or without collaboration with DCS).
- Systems / applications developed and maintained by contractors and COTS or GOTS products.
- Systems / applications that process, store and / or transmit SSA data.

The Component Security Officer (CSO), under the authority of the Deputy Commissioner for Systems, may conduct periodic audits and / or random tests of procedures and data custodianship practices.

### **3.6.1.1 Audit Trail Requirements**

Information systems are vital to the SSA's mission / business processes; therefore, securing the confidentiality, integrity, and availability of the information processed by agency Information System becomes extremely important. One of the key tools used in accomplishing these objectives is the Information System "audit trail".

An audit trail collects and maintains a record of events performed to assist in deterring, detecting, and investigating instances of suspected fraud and abuse. The SSA security requirements are driven by Federal security requirements which are mandated and directed by (but not limited to) FISMA, and the National Institute of Standards and Technology (NIST). It is agency policy that an audit trail is required for any system that:

- Allows querying of, or displays, sensitive information for which a risk assessment determines that a threat exists and information could be misused and lead to fraud or abuse of SSA systems.

- Processes changes to information on SSA systems for which a risk assessment determines that a significant threat exists, if the ability to make these changes could be misused and lead to fraud or abuse of SSA systems.
- Stores SSN level data on a database rather than a mainframe (i.e., “data at rest”) and the user has the ability to query this data from the application.

The Application development teams must consider the need for an audit trail from the beginning of a project’s development lifecycle and for each subsequent release. The development teams working through their ISOs, in consultation with OIS and CSOs, must conduct a quantitative assessment of the risk to the data in their applications to determine the need for an audit trail.

When an audit trail is required, audit records must, at a minimum, capture the following information:

- The account used to access data or effect an action (i.e., PIN for internal users, Internet Protocol (IP) address from where the transaction originated for internet applications).
- The date and time data was viewed or changed.
- The geographic (physical) location from which data was accessed.
- The type of action taken (e.g., access data, file a claim, change an address).
- Any other data elements accessed or affected by the action that a risk assessment determined will be valuable to investigate for potential fraud or abuse.
- Sensitive information provided by internet users such as their passwords and answers to personal security questions should not be maintained in the audit record.

Only OIS can approve further exceptions to the following restrictions:

- All audit trail data must be securely maintained to protect confidentiality and ensure data integrity and availability.
- Unauthorized access to audit trail data is prohibited.
- The unauthorized modification of audit trail, once captured, is prohibited.
- Audit trail data stored outside of official repositories should be securely destroyed after it is no longer required for the original purpose.

#### **3.6.1.1.1 Use of Audit Data**

The use of audit trail data to measure user performance (i.e., the quantity and quality of work) is prohibited. Audit trail data can only be used to obtain:

- Evidence of suspected abuse or fraud.
- Evidence of suspicious activity related to a specific incident.
- Documentation in support of security or integrity reviews, or
- Evidence of patterns of suspicious system use.



### 3.6.1.1.2 Distribution of Audit Data

Distribution of audit trail data is restricted to security staff in OIS, Office of Quality Review (OQR), DCO/Office of Public Service and Operations Support (OPSOS), OIG, the regional offices, Program Service Centers (PSC), ODAR, OSOHE, CSOs and SOs within their respective applications. Audit trail data can be shared and / or reviewed with management in support of investigations. Only OIS can approve further waivers to these restrictions (See [ISP Appendix A, Requests for Waivers from Information Security Policy \(ISP\) Policies](#), and [ISP 3.2.2, Role-based Training for Personnel with Significant Cybersecurity Responsibilities](#) for more information).

### 3.6.1.1.3 Audit (b) (7)(E) Core Services

The Audit (b) (7)(E) Core Service facilitates the auditing requirements for distributed applications that contain "data at rest". The term "data at rest" is commonly used at SSA for data that has been exported or downloaded from mainframe repositories. If this data at rest is viewed by someone other than the person who originally downloaded, exported or screen-scraped it from the mainframe, and if the data is SSN specific, the Audit (b) (7)(E) Core Service should be used. Web developers may choose to use the Audit (b) (7)(E) Core Service to meet auditing requirements. Further information about Audit (b) (7)(E) Core Service can be found at the [Audit Core Service](#) site.

### 3.6.1.1.4 Additional Audit Coverage Areas

Policy listed in previous sections focused on "user activity" as it relates to fraud, abuse, etc. performed within SSA systems. Additional audit coverage areas within an Information System can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events (actions that happen on a computer system), intrusion detection, and problem analysis.

### 3.6.1.1.5 System-Level

System-level audit and log records are used to monitor and fine-tune system performance. The system itself enforces certain aspects of policy (particularly system-specific policy) such as access to files and access to the system.

### 3.6.1.1.6 Application Level

Application audit trails are used to discern flaws in applications, or violations of security policy committed within an application. Based on the risk assessment of the Information System, sometimes a finer level of detail than system audit trails is required.

### 3.6.1.1.7 Individuals of Extraordinary National Prominence (IENP) and Own SSN Requirements

SSA employees, contractors and data sharing partners using SSA systems are prohibited from accessing the following:



- Records belonging to IENP
- Their own SSN
- Any record where their SSN is present

All internal SSA applications that access client data must implement both the IENP and Own SSN Blocks, or ensure that the blocks have been previously implemented by another application.

The following information needs to be captured when the IENP and Own SSN Blocks are implemented:

- SSN
- Employee PIN
- Invoking Application Name
- Time and Date of Violation
- Location of Violation
- Office Name

For external applications (i.e., those requests from parties outside of SSA), the response code to requests for IENP records must protect the sensitivity of the record and not produce messages that could be used to infer the sensitive nature of the record. In the event of special circumstances that may involve not implementing the IENP and Own SSN blocks, please refer to [ISP Appendix A, Requests for Waivers from Information Security Policy \(ISP\) Policies](#) for submitting a waiver request. Additional information regarding IENP can be found in the [Program Operating Manual System \(POMS\) TC 01001.023 Restricted Records](#).

### **3.6.2 System Logging Requirements**

All applications and devices that handle information must record and retain event-logging information sufficient to answer the following questions:

- Who or what did the action or activity?
- What activity or action was performed?
- What application or device the action or activity was performed from or on?
- What the action or activity was performed on (the object)?
- When was the action or activity performed?
- What was the status, outcome, or result of the action or activity (such as success vs. failure)

#### **3.6.2.1 Logged Events**

- Logged events must adhere to the specific security guide for each authorized platform on SSANet.

- Unless otherwise specified in the configuration guide, the [General Logging Requirements](#) must be applied. For event log elements and requirements for different data types refer to the Information Security Configuration Guide .
- Application or device specific events to be logged must be identified in the system's Audit Plan.

### **3.6.2.2 Event Log Elements**

Event logs must identify or contain at least the following elements, directly or indirectly (inferred).

1. Type of action – such as authorize, create, read, update, delete, and accept network connection.
2. Subsystem performing the action – such as process or transaction name, or identifier code.
3. Identifiers for the subject requesting the action – such as user name, system or host name, IP address, and MAC address.
4. Identifiers for the object the action was performed on – such as file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address.
5. Date and time must be configured in Universal Time Coordinated (UTC).
6. Whether the action was allowed or denied by access-control mechanisms.
7. Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

### **3.6.2.3 Log Review and Update**

Application and device owners must:

- Review log files and dashboard summaries as specified in the Information Security Configuration Guide.
- Review the event logging capture requirements on at least an annual basis, and update as necessary.

### **3.6.2.4 Event Log Access**

Access to event logs must be restricted using least privilege and need to know.

### **3.6.2.5 Log Format and Storage**

The application or device must support the formatting and storage of event logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting.

Event logs must be sent to the agency centralized log collection system.

Contact the Security Operations Center at (b) (7)(E), (b) (7)(C) for initial log setup, storage, and alerting guidance.

### 3.6.2.5.1 File Integrity Check Required

(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)

### 3.6.2.5.2 Retention

SSA utilizes the [General Records Schedule \(GRS\) 3.2, item 010](#), for all event logging records. Records should be retained as per the period guidelines defined in the SSA Log Requirements tables but can be modified as dictated by business needs. SSA utilizes the General Records Schedule (GRS) 3.2, item 031, for all audit trail data / records. Furthermore, the SAM and / or SO must utilize the audit plan as the authoritative source for defining system specific audit trail data / records retention period(s).

For records retention, component management must follow the established SSA [record retention schedules](#) for all information security-related training records.

### 3.6.2.5.3 Categorization

All systems must be categorized based on the type of data processed by the information system and the system categorization level.

### 3.6.2.5.4 Requirements

(b) (7)(E)

(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)

(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)

(b) (7)(E)

(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)

### 3.6.2.5.5 Definitions

**Online data** – System, management, or network log data maintained locally on the server or device

**Offline data** – System, management, or network log data transferred to a central analysis system or offline/archive storage location (tapes)

**Sensitive data** – Sensitive Information. Information protected from unauthorized disclosure. Includes, but is not limited to, Personally Identifiable Information (PII), Federal Taxpayer Information (FTI), and SSA proprietary business data (source: [ISP Section 3.3.2.4](#))

**Impact System** – Categorization of systems based on implemented security controls that

evaluate the potential impact a loss of confidentiality, integrity, or availability would have on operations, assets, and/or individuals associated with SSA. (source: [ISP Section 2.1.3](#))

### **3.6.3 Removable Media and Protection from Data Loss Policy**

#### **3.6.3.1 Removable Media Devices**

Removable media must be protected in accordance with the following policy:

- The storage of SSA information is prohibited on removable media unless it is required in the performance of one's official duties.
- SSA information stored on removable media must only be accessed using an SSA owned resource.
- Any non-SSA procured removable media devices including, but not limited to, Universal Serial Bus (USB) drives, Compact Disks (CDs), Smartphones, Digital Versatile Disks (DVDs), floppy disks, or other devices with data storage capacity are prohibited from being connected to any SSA owned resource. This includes connecting devices for charging them through a USB connection.

This policy applies to all circumstances with the exception of the allowable instances mentioned below:

- Removable media received from the public containing information used for claims processing, programmatic, or other authorized business purposes is allowable, provided the following conditions are met:
  - Up-to-date automatic antivirus and data loss prevention software must be installed and operational on any workstation that is used to read removable media from the public.
  - Auto-run capabilities on SSA Information Systems must be disabled.

#### **3.6.3.2 Data Loss Protection**

Data Loss Prevention (DLP) is implemented using various techniques and mechanisms.

Policy for data loss prevention include:

- [ISP 3.4.6 Media Sanitization](#) contains requirements to protect sensitive information stored on mobile devices and removable media.
- When removing Information Technology (IT) equipment, such as workstations or servers, from SSA facilities, sensitive information must be encrypted or protected from compromise, unauthorized modification, or loss.
- Ensure that files containing sensitive information are identifying to the Local Access Network (LAN) Manager or appropriate personnel to facilitate backup.

- In the event, that access to the building is prohibited. Maintain backup media at a remote SSA-approved site with reasonable access and restoration time to ensure availability.
  - [Administrative Instructions Manual \(AIMS\), Material Resources Manual, Section 07.06](#) defines long-term records storage requirements.
- Store media containing sensitive information in a secure location when not in use, and properly dispose of when no longer needed ([ISP 3.3.4 IT Equipment Safeguards](#)).

For more information about the SSA DLP program, please visit DSE's [Data Loss Prevention website](#).

### **3.6.3.3 Local Manager Responsibilities**

The local Manager is responsible for enforcing the following policies:

- Secure SSA-owned removable media.
- Ensure that mobile computing devices are secure when not in use (e.g., hand-held PCs, Smartphones, USB flash drives, etc.).
- Ensure that all critical information and applications residing on LAN servers are backed-up regularly

### **3.6.4 Access Enforcement**

System owners must ensure access to systems and assets is controlled by incorporating the principle of least privilege as discussed in [ISP Section 3.1.3.1 Access Management](#), and the principle of least functionality.

The principles of least functionality are met by configuring the information system to provide only essential capabilities. The use of unauthorized functions, ports, protocols, and services are prohibited. Systems must be configured in compliance with applicable Security Configuration Standards.

For comprehensive access enforcement, all SSA information system must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies as defined in [Section 3.1](#).

### **3.6.5 Communication and Control Network Protection**

#### **3.6.5.1 Network Boundary Protection**

Firewalls must protect the SSA network(s). The firewall protection strategy, including firewall placement configuration and monitoring is described in a separate document entitled (b) (7)(E) (b) (7)(E). The (b) (7)(E) document is restricted to a limited audience on a (b) (7)(E) basis.

### 3.6.5.2 Network Control Devices

Network control devices include routers, switches, and hubs that allow devices to connect and communicate within a Local / Wide Area Network (LAN / WAN) environment. Unauthorized modification or access to any device configuration is prohibited. Network devices must meet the following configuration standards:

- (b) (7)(E), (b) (2) [Redacted]

- (b) (7)(E), (b) (2) [Redacted]

[Redacted]

(b) (7)(E), (b) (2)

[Redacted]

### **3.6.5.3 Peer-to-Peer (P2P) and Web Conferencing / Collaboration Technologies**

The use of P2P (file sharing) technology is prohibited. Such technologies are susceptible to malware, and could expose the agency to increased cyber threats.

Web conferencing, or collaborating, within the SSA network is authorized only via the agency-approved collaboration solution. All other forms of web conferencing solutions, including webcasting, collaboration, and webinar technologies, are prohibited from use within SSA's network environment.

### **3.6.5.4 Instant Messaging**

Instant Messaging (IM) within SSANet is authorized only via the agency-approved IM solution. All other forms of IM solutions are prohibited from use within SSA's network environment.

SSA CONFIDENTIAL INFORMATION



## 4 Section IV: Detect

This section provides the Information Security policy for developing the organizational understanding to identify the occurrence of a cybersecurity event. It includes the following categories.

- Anomalies and Events (DE.AE);
- Security Continuous Monitoring (DE.CM); and
- Detection Processes (DE.DP)

### 4.1 Anomalies and Events

This section provides governance on how anomalous activity is detected, the timeframes in which detection will take place, and how the impact of the event will be established and managed.

#### 4.1.1 Network and Security Operations

SSA must have the capability to detect potential malicious activity on SSA systems. The SSA Division of Security Operations (DSO) has the primary responsibility for security operations. DSO functions include the following:

- Incident Handling
- Vulnerability Assessment
- Compliance Monitoring
- Situational Awareness
- Network Intrusion Detection Services
- Forensic Services

The SSA DSO monitors SSA systems in order to:

- Detect indications of potential attacks in accordance to SSA policy;
- Detect unauthorized local, network, and remote connections; and
- Identify unauthorized use of SSA systems

DSO personnel are required to protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

When applicable, DSO personnel obtain legal opinion from OGC with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

Monitoring information is provided to designated personnel as needed.

## 4.1.2 Security Event Analysis and Response

SSA uses risk assessments to determine the impact and likelihood of risks associated with an IT system (or data) throughout the SDLC. The output of this process helps identify appropriate controls for reducing or mitigating risk during the risk mitigation steps.

For detailed description on the Risk Management Framework, see NIST SP 800-37, “Guide for applying the Risk Management Framework to Federal Information Systems”.

In addition, SSA approaches risk management by using Federal guidelines provided for risk assessment in NIST SP 800-30, “Guide for conducting Risk Assessments”.

### Detecting Violations

All employees should be aware of the following Agency tools available to management for use to detect criminal violations.



- **Audit Trail System (ATS)** – The ATS monitors SSA systems and collects information based on transactions entered by individual systems users. It provides information to support the investigation of individuals suspected of fraud.



## 4.1.3 Reporting

SSA’s incident reporting process requires agency information system users to report any activities that may compromise the confidentiality, integrity, or availability of agency information or Information Systems.

**Reporting Suspected Incidents:** Any user observing a suspected systems intrusion attempt or other security-related incident, such as suspicious email (phishing) or suspicious phone call (vishing), must report the incident to the (b) (7)(E), (b) (2)

## **NOTE**

*When reporting suspicious phone calls or emails, please follow the reporting procedures outlined on OIS' [Social Engineering Resources](#) page.*

**(b) (7)(E), (b) (2)**

responsibilities and to the US-CERT as soon as it determines that a major incident is occurring.

### **4.1.3.1 Incidents Relating to Program and Employee Fraud**

All SSA employees must follow the procedures for detecting and reporting suspected program and employee fraud is found in the Program Operating Manual System (POMS) [GN 04111](#) and [GN 04112](#). Employees can report suspected program fraud cases to their supervisors or through the Fraud hotline maintained by the OIG. The SSA Fraud hotline number for reporting alleged or suspected employee and program violations is 1-800-269-0271. SSA employees may also report potential program violations via the electronic form [E8551- Reporting Form for Programmatic Fraud](#). Do not use this form, however, for alleged employee violations.

### **4.1.3.2 Reporting Loss of Personally Identifiable Information (PII)**

Policy and instructions for reporting the loss of PII are located in Administrative Instructions Manual System (AIMS) General Administration Manual (GAM) Chapter 15, Instruction 2, Personally Identifiable Information (PII) Loss and Remediation, Reporting the Loss of PII. [AIMS 15.02](#) is the definitive source of information concerning PII loss reporting.

### **4.1.3.3 Reporting Unauthorized Federal Tax Information (FTI) Access or Improper FTI Disclosure**

SSA must notify IRS within 24 hours of an improper access or disclosure of FTI. Components that experience unauthorized access of FTI or its improper disclosure must report it to OIS. At a minimum, the report should include the information below. However, do not delay making a timely report to OIS to fully satisfy the informational requirements.

- Component name and Point of Contact (POC)
- Date and time of the incident
- Date and time of discovery
- How the incident was discovered
- Description of the incident and data involved
- Potential number of records involved (if unknown, provide a range)
- IT involved (e.g., laptop, server, mainframe)

Send inquiries or questions concerning the content of this IRS FTI safeguard issues to **(b) (7)(E), (b) (2)**

**(b) (7)(E)**

#### **4.1.3.4 Criminal Violations and Fraud Policy**

SSA employees must be able to identify Information Security violations within the scope of their job and are required to report those suspected violations. Any violation of the Social Security Act or relevant sections of the Federal Criminal Code is considered criminal when it is a material act, done knowingly, willfully, and with intent to defraud. SSA's OIG investigates allegations of criminal violations. Employees should contact their Manager and / or the OIG when in doubt as to whether to report a suspected violation. The following definitions are helpful in determining when to report suspected Information Security violations:

- **Material** – The point at which a false statement, representation, or deceitful withholding of information, under a legal obligation to disclose the truth, (a) influences payment of benefits not authorized by the Social Security Act, (b) influences SSA in determining rights to payments, or (c) leads to the improper issuance of Social Security Number (SSN) cards or other documents.
- **Knowingly** – Performing a particular act while knowing the act is unlawful.
- **Willfully** – Voluntarily, purposefully, deliberately, and intentionally, while knowing of a legal obligation, evading that obligation.
- **Intent to Defraud** – Making a representation one either knows or believes to be false, while knowing that the misrepresentation could lead to some unauthorized (fraudulent) benefit to oneself or to some other person; intentional deception.

In addition to information in this subsection, instructions for SSA employees to report suspected fraud and / or criminal violations are found in [POMS](#) (see POMS in References).

Examples of potential employee violations can also be found at [POMS GN 04112.005](#), Reporting Employee Criminal Violations – General.

##### **4.1.3.4.1 Violations Reporting Process**

CSOs and Regional Center Directors for Security and Integrity (CDSI) report incidents for their respective components and where appropriate, work with other components to resolve incidents. If an employee identifies or detects a suspected criminal violation, he / she must report the incident (see the POMS [GN 04111](#) and [GN 04112](#)).

##### **4.1.3.4.2 Programmatic Violations**

SSA employees must report alleged or suspected program violations directly to the OIG/Office of Investigations (OI), using the electronic form [e8551](#), within (b) (7)(E), (b) (2) after detection.

Employees should use this form, available on the [OIG Website](#), only for alleged or suspected program violations. The procedure for reporting potential program violations depends on where the potential fraud is discovered (see POMS [GN 04111.010 -.040](#)).

#### **4.1.3.4.3 Employee Violations**

SSA employees must report alleged or suspected employee violations to the OIG / OI. The procedure for reporting potential employee violations depends on whether the reporting employee is a non-managerial employee or a member of management (see [POMS GN 04112.015](#) – How Employees Report Employee Criminal Violations).

#### **4.1.3.4.4 SSA Fraud Hotline**

Information about the OIG Allegation Management Division (AMD) Fraud Hotline and guidelines for reporting violations are found on the [OIG Website](#). The OIG maintains and operates the SSA Fraud Hotline (also identified as AMD) for the public to report alleged or suspected program and employee violations. Employees who wish to report suspected employee violations should [follow POMS GN 04112.015](#) – How Employees Report Employee Criminal Violations.

#### **4.1.3.4.5 Request for Assistance by SSA OIG**

SSA OIG investigates allegations of criminal violations and if appropriate, prepares cases for criminal prosecution, civil suit, and administrative sanctions. OIG / OI compile all requests for information pursuant to an investigation. Report the suspected violation and assist the [OIG Field Division](#) in the development of violations; provide testimony, and other support for OIG investigations of SSA violations.

#### **4.1.3.4.6 Request for Information by Other Law Enforcement Agencies and Investigators**

Requests for information made by other law enforcement agencies and investigators including cases involving national security must be processed according to the instructions provided in [POMS GN 03312.001](#) – Disclosure without Consent for Law Enforcement Purposes. Direct any questions about disclosure of information to the appropriate regional or component privacy coordinator.

## **4.2 Security Continuous Monitoring**

This section provides policy to ensure information systems and assets are monitored at discrete intervals to identify cybersecurity events, and addresses how the agency verifies the effectiveness of protective measures.

### **4.2.1 Personnel Activity Monitoring**

#### **4.2.1.1 Email and Fax Monitoring**

The SSA Logon Security Warning banner states that all users see and agree to prior to logging on to an agency system. SSA considers email and Fax messages to be government property ([OPLM Email Retention Policy](#)), and reserves the right to record, review, audit, intercept, access, delete, and disclose all messages received, sent, or printed over SSA systems. SSA follows

Federal law and NIST standards and guidelines, which allow it to monitor Fax or email transmissions without prior notice.

#### **4.2.2 Malicious Code Detection**

SSA has various security controls in place to protect the agency's information from alteration, destruction, loss, or disclosure. This includes the implementation of tools to detect and remediate potential Malicious Code events.

#### **4.2.3 Service Provider Monitoring**

ESPs deliver outsourcing of systems / network operations, telecommunication services, or other managed services. All organizations that transmit, process, or retain SSA information, or use SSA Information Systems, are responsible for following the same Security Assessment and Authorization (SA&A) process as those systems housed internally. See the [SA&A webpage](#) for more information on the SA&A process. For additional requirements regarding External Service Providers, see the [ESP Procurement Page](#).

#### **4.2.4 Monitoring for Unauthorized Connections, Devices, and Software**

The DSO monitors SSA networks for unauthorized connections, devices and software as a component of the SSA Continuous Diagnostics and Mitigation (CDM) and compliance monitoring programs.

#### **4.2.5 Vulnerability Scanning**

Vulnerability scans are performed on a periodic basis by the SSA DSO Team and in support of the SA&A activities.

## 5 Section V: Respond

This section outlines the agency's policy for responding to a detected cybersecurity event. It includes the following categories.

- Response Planning (RS.RP);
- Communications (RS.CO);
- Analysis (RS.AN); and
- Mitigation (RS.MI)

### 5.1 Response Planning

SSA's Information Security Program requires an ongoing agency process to monitor, detect, eliminate, mitigate, and report significant Information Security incidents and risks of physical and cyber-attacks on SSA's network infrastructure and to protect our systems and information.

The SSA DSO performs strategic analysis, issues warnings/alerts, and coordinates response and recovery efforts related to threats against SSA information and Information Systems. The agency must:

- Have an incident response process for responding to significant attacks with the goal of isolating and minimizing damage. The incident response process must:
  - Include Information Security incident reporting capability.
  - Enable sharing of information with other organizations, consistent with NIST guidelines.
  - Assist the agency in pursuing appropriate legal action, consistent with Department of Justice (DOJ) guidance.
  - Provide timely technical assistance to agency Information System operators to include guidance for:
    - Detecting and handling Information Security incidents.
    - Compiling and analyzing information regarding incidents that threaten agency assets.
    - Notifying Information System operators of current and potential Information Security threats and vulnerabilities.

### 5.2 Communications

This section provides policy on response activities which are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

## 5.3 Analysis

The following subsections provide policy for analyzing security events, and incidents to ensure adequate response and support for recovery activities.

### 5.3.1 Security Event Notification

Upon receiving notification of a security event, Incident Response or DSO personnel must notify appropriate stakeholders, in accordance with Incident Response Plans, to begin sharing information needed to effectively analyze the event. Stakeholders include operators of agency information systems.

### 5.3.2 Impact Analysis

The DSO compiles and analyzes security event and incident information to determine the impact to SSA information and Information Systems.

## 5.4 Mitigation

The following subsections provide policy to ensure activities are performed to prevent expansion of an event, mitigate its effects and eradicate the incident.

### 5.4.1 Incident Handling

Cybersecurity incidents are handled in accordance the SSA Cybersecurity Incident Response and Recovery Plan. This plan includes processes for incident handling across lifecycle of the incident, including:

1. Preparation;
2. Identification;
3. Containment;
4. Eradication;
5. Recovery; and
6. Lessons Learned

### 5.4.2 Information Sharing and Reporting

Information related to cybersecurity events and incidents are shared as described in [ISP Section 5.1, Response Planning](#). In addition, newly identified vulnerabilities are mitigated or documented as accepted risks.



## 6 Section VI: Recover

This section provides Information Security policy for maintaining plans for resilience and to restore capabilities that were impacted due to a cybersecurity event. It includes the following categories.

- Recovery Planning (RC.RP); and
- Improvements (RC.IM)

### 6.1 Recovery Planning

SSA systems must recover and reconstitute to a known state after a disruption, compromise, or failure due to a cybersecurity event. Additionally, information systems that are transaction-based must implement transaction recovery if a cybersecurity event occurs.

SSA implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication and recovery.

#### **NOTE**

*For more information on SSA's policy in relation to Recovery Planning, please refer to Contingency Planning ([Section 2.2.2](#)) and Incident Response ([Section 3.4.8](#))*

### 6.2 Improvements

The system owner must coordinate incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, testing and implementation.


#### **NOTE**

*For more information on SSA's policy in relation to Improvement, please refer to Contingency Planning ([Section 2.2.2](#)) and Incident Response ([Section 3.4.8](#))*

## 7 Section VII: Appendices

### Appendix A: Requests for Waivers from Information Security Policy (ISP) Policies

(b) (7)(E), (b) (2)



(b) (7)(E), (b) (2)

SSA CONFIDENTIAL INFO



(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

CONFIDENTIAL INFORMATION

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E), (b) (2) [Redacted]

(b) (7)(E), (b) (2) [Redacted]

[Redacted]

(b) (7)(E), (b) (2)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E), (b) (2)

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

(b) (7)(E), (b) (2)

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



(b) (7)(E), (b) (2)

|

|

|

|

|

|

|

|

|

|

|

|

|

(b) (7)(E), (b) (2)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E), (b) (2)

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]

[Redacted text block]

[Redacted text block]

(b) (7)(E), (b) (2)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E), (b) (2) [Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

(b) (7)(E), (b) (2)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E), (b) (2) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E), (b) (7)(D)

[REDACTED]

[REDACTED] ACTING  
(b) (7)(E)



(b) (7)(E), (b) (2)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E)



(b) (7)(E), (b) (2)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E), (b) (2)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E), (b) (7)(D)

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

(b) (7)(E)

(b) (7)(E), (b) (2)

[Redacted text block]

[Redacted text block]

[Redacted text block]

(b) (7)(E), (b) (2)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E), (b) (2)

[Redacted text block]

[Redacted text block]

[Redacted text block]

(b) (7)(E), (b) (2)

[Redacted text block]



(b) (7)(E), (b) (2)

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

(b) (7)(E), (b) (2)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E), (b) (2)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E), (b) (2)