Description of document:	Three (3) Social Security Administration (SSA) Information Security policy documents, 2001-2017
Requested date:	03-January-2017
Released date:	25-April-2018
Posted date:	28-May-2018

Records included:

- Information Security Policy (ISP) for the Social Security Administration (SSA) Handbook, 2017
- Rules of Behavior for Users and Managers of SSA's Automated Information Resources, 2001
- Systems Sanctions Violations - Agency Policy and Acknowledgement Statement, 2009

Source of document:

CDC/ATSDR
Attn: FOIA Office, MS-D54
1600 Clifton Road, NE
Atlanta, GA 30333
Fax: (404) 235-1852
Email: FOIARequests@cdc.gov

SOCIAL SECURITY

Refer to:
S9H: AR3090

April 25, 2018

I am responding to your January 3, 2017 Freedom of Information Act (FOIA) request for an electronic copy of the Information Systems Security Handbook, the Rules of Behavior for Users and Managers of SSA's Automated Information Resources, and a memorandum entitled "Sanctions for Unauthorized Systems Access Violations and Guidance for Employees on How to Transact Social Security Business that Requires System Access."

We located 169 pages of responsive records. I am releasing 140 pages in full and 29 in part, pursuant to FOIA exemptions 6 and 7(E). All CDs created by SSA are automatically encrypted. Since these documents are not relating to someone in particular, we can include the password in this letter. The password for the disc is: P@ssw0rd=1.

When we receive a request from a member of the public to release personal information about another individual from our records, we must balance the individual's privacy interest in withholding the information against the public interest in disclosing the information. We must determine whether disclosure would affect a personal privacy interest. Individuals clearly have a substantial personal privacy interest in the personal details furnished to the government. On the other hand, the only public interest we must consider is whether the information sought would shed light on the way an agency performs its statutory duties. We may not consider the identity of the requester or the purpose for which the information is requested. While the public has an interest in knowing how the Social Security Administration administers the Social Security Act, disclosing records containing personal information about named individuals would not shed light on how the agency performs its statutory duties. Therefore, disclosing this information would be a clearly unwarranted invasion of personal privacy, and the FOIA (5 U.S.C. § 552(b)(6)) does not require disclosure.

I am withholding information related to the agency's physical security practice under FOIA Exemption 7(E) (5 U.S.C. § 552(b)(7)(E)). Exemption 7(E) exempts from mandatory disclosure records or information compiled for law enforcement purposes when production of such records "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law."

If you have questions, or would like further assistance with your request, you may contact our FOIA Public Liaison by email at FOIA.Public.Liaison@ssa.gov; by phone at 410-965-1727, by choosing Option 2; or facsimile at 410-966-0869.

You may also contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration for dispute resolution services. OGIS is an entity outside of the Social Security Administration that offers mediation services to resolve disputes between FOIA requesters and Federal agencies. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road – OGIS, College Park, MD 20740-6001; email at ogis@nara.gov; telephone at 202-741-5770; toll-free at 1-877-684-6448; or facsimile at 202-741-5769.

If you disagree with this decision, you may file a written appeal with the Executive Director for the Office of Privacy and Disclosure, Social Security Administration, 617 Altmeyer Building, 6401 Security Boulevard, Baltimore, Maryland 21235. Your appeal must be postmarked or electronically transmitted to FOIA.Public.Liaison@ssa.gov within 90 days of the date of our response to your initial request. Please mark the envelope or subject line with "Freedom of Information Appeal."

Sincerely,

Monica Chyn
Acting Freedom of Information Officer

Enclosure

INFORMATION SECURITY

POLICY (ISP)

FOR

THE SOCIAL SECURITY ADMINISTRATION (SSA)

OFFICE OF INFORMATION SECURITY

RELEASED JUNE 6, 2017

VERSION 6.0

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	04/01/2014	Draft Version	(b) (6)	XX/XX/XXXX (2 digit month, 2 digit day, 4 digit year)	(first initial, last name, and office symbol in parentheses)	XX/XX/XXXX (2 digit month, 2 digit day, 4 digit year)
1.1	11/02/2015	Update to section 2.1.1.3 to include requirements that windows service accounts be placed in proper AD group and that service accounts only be used for the assigned purpose. Update to section 2.1.1.4 to include requirements that privileged users use their standard account when possible, access rights be removed when the account is disabled, and access rights reviewed whenever there is a role change. Added links to an Account Type table providing additional information.	(b) (6)	10/30/2015	(b) (6)	11/02/2015
1.2	11/10/2015	Update to section 2.1.3 and to 2.5.4 to remove references to SSA-120 and SSA-119, added reference to (b) (7)(E) portal. Update to section 5.3.1.9 to correct hyperlink to the August 2015 version of the Security Audit Reports manual.	(b) (6)	11/10/2015	(b) (6)	11/13/2015

1.3	01/14/2016	Maintenance modifications to various sections including minor word changes, typo corrections, and hyperlink corrections.	(b) (6) [redacted]	01/14/2016	(b) (6) [redacted]	01/14/2016
1.4	02/01/2016	Minor word changes to Waiver Request Form to reflect change from ISSH to ISP. Added acceptance of electronic signature in Instructions for Completing the Waiver Request Form.	(b) (6) [redacted]	02/01/2016	(b) (6) [redacted]	02/01/2016
1.5	02/24/2016	$ID moved to General User Account in Account Type Matrix Table linked from Section 2.1.1.3. Changed ^SPAM Help mailbox to ^SOC mailbox. Changed "employees can" to "employees must". Corrected an ISP section reference. Corrected link referral to OIG homepage.	(b) (6) [redacted]	02/24/2016	(b) (6) [redacted]	02/24/2016
1.6	02/26/2016	Identified a location to track SSA Cloud Systems list and added requirement of approval from the OIS CIO and OAG.	(b) (6) [redacted]	02/26/2016	(b) (6) [redacted]	02/26/2016
1.7	03/03/2016	Updated Systems component formerly the Office of Telecommunications and Systems Operations (OTSO) to the Office of Systems Operations and Hardware Engineering (OSOHE) throughout the ISP.	(b) (6) [redacted]	03/03/2016	(b) (6) [redacted]	03/03/2016
1.8	03/04/2016	Updated Section 6.3.3 to name (b) (7)(E) [redacted] as current media encryption software. Repaired the link to the corresponding user instructions.	(b) (6) [redacted]	03/04/2016	(b) (6) [redacted]	03/04/2016
1.9	03/16/2016	Updated third paragraph of Section 3.3.2 to clarify the responsibility of contractors and other non-SSA employees to complete travel request form.	(b) (6) [redacted]	03/16/2016	(b) (6) [redacted]	03/16/2016

2.0	03/18/2016	Corrected NIST reference in Section 4.2.4.7 from F4, Ongoing Authorization to F6, Event-Driven Triggers.	(b) (6)	03/18/2016	(b) (6)	03/18/2016
2.1	03/21/2016	Updated Section 5 to modify link from OIS Home page to OIS Incident Response page.	(b) (6)	03/21/2016	(b) (6)	03/21/2016
2.2	03/29/2016	Renamed section 2.5 to 'References' and deleted Section 2.1.3 because links already exist in Section 2.5.4.	(b) (6)	03/29/2016	(b) (6)	03/29/2016
2.3	04/25/2016	Corrected grammatical error in bullet list in Section 5.1.1 and removed broken FTP waiver procedure link in Section 4.6.3.1.	(b) (6)	04/25/2016	(b) (6)	04/25/2016
2.4	04/28/2016	Updated broken NIST link in Access Control definitions in Section 2.1.3.	(b) (6)	04/28/2016	(b) (6)	04/28/2016
2.5	05/03/2016	Updated Section 2.1.1.4 to specify that Active Directory Enterprise and Domain administrator accounts must not have access to the internet.	(b) (6)	05/03/2016	(b) (6)	05/03/2016
2.6	05/11/2016	Updated definitions of policy, standards, guidelines, procedures, and process in Section 1.3.	(b) (6)	05/11/2016	(b) (6)	05/11/2016
2.7	05/12/2016	Modified Section 4.3.2.1 to specify that the agency's SDLC is a policy that applies to the development of software tools and applications.	(b) (6)	05/12/2016	(b) (6)	05/12/2016

2.8	05/13/2016	Modified Section 3.4.5 by eliminating specific steps taken by OIS during the exception process.	(b) (6)	05/13/2016	(b) (6)	05/13/2016
2.9	05/17/2016	Updated Section 4.2.2 to clarify that risk management is policy not procedure by removing the word “phase” from the list of SDLC risk management components.	(b) (6)	05/17/2016	(b) (6)	05/17/2016
3.0	05/26/2016	Modified Section 6 to address internal data management requirements, security objectives, and define data and data custodianship. Made minor word changes in Section 4. Deleted Data Owner definition and updated Data Custodian definition.	(b) (6)	05/26/2016	(b) (6)	05/26/2016
3.1	05/31/2016	Updated Section 4.2.3 by listing the Risk Management Framework (RMF) component identified in NIST as elements and not procedural steps.	(b) (6)	05/31/2016	(b) (6)	05/31/2016
3.2	06/03/2016	Corrected NIST reference in Section 4.5.2.3 to NIST SP 800-53 Rev. 4 (April 2013), Security and Privacy Controls for Federal Information Systems and Organizations.	(b) (6)	06/03/2016	(b) (6)	06/03/206
3.3	06/09/2016	Modified Section 2.1.1.3 by clarifying the timeframe of account suspension for terminated or separated employees and contractors per HSPD-12 guidelines. Added links to ISP Manual and AIMS to reference how a manager requests removal of access to information system accounts.	(b) (6)	06/09/2016	(b) (6)	06/09/2016
3.4	06/20/2016	Corrected link in Section 5.2.1.2 so that it directs to Administrative Instructions Manual (AIMS) Chapter 15.	(b) (6)	06/20/2016	(b) (6)	06/20/2016

3.5	06/22/2016	Inserted link to encryption standards in Section 6.3.1.	(b) (6)	06/22/2016	(b) (6)	06/22/2016
3.6	06/23/2016	Corrected NIST reference format throughout the ISP.	(b) (6)	06/23/2016	(b) (6)	06/23/2016
3.7	06/30/2016	Updated phishing reporting instructions in Section 5.2.1.1 by directing users to email ^SOC upon receipt of a suspicious email. Also added instructions on reporting vishing/suspicious phone calls.	(b) (6)	06/30/2016	(b) (6)	06/30/2016
3.8	07/01/2016	Re-inserted sentence concerning approval of wireless pointing devices that was inadvertently deleted.	(b) (6)	07/01/2016	(b) (6)	07/01/2016
3.9	07/08/2016	Modified Appendix B by updating a reference to Chapter 21 of the Information Systems Security Handbook (ISSH) to Section 5.3.1.7 of the ISP.	(b) (6)	07/08/2016	(b) (6)	07/08/2016
4.0	07/20/2016	Corrected broken (b) (7)(E)) and (b) (7)(E) 4009 links in Section 2. Corrected broken Systems Security Assessment and Authorization (SSA&A) links in Section 3.	(b) (6)	07/20/2016	(b) (6)	07/20/2016
4.1	09/14/2016	Modification to Section 3.2.1 was made by inserting a note to clarify the need for an exception when the wireless pointing device requires additional software. Modification to Section 4.1.2 involved removing the procedural steps involved in risk management and risk assessment.	(b) (6)	08/18/2016	(b) (6)	09/16/2016

		Updates to Section 4.4.2.1 were made by restructuring the language to specify the need for development teams to conduct an assessment of the risk to the data in their applications to determine the need for an audit trail. Modified Section 4.5.1.1 by removing the procedure for completing the required artifacts related to the Security Authorization Process. Links to the instruction were added for reference. Changes were made to Section 5.2.2.2 to specify that employees must follow the procedures for detecting and reporting suspected program and employee fraud. Modification to Section 6.2.1 involved adding floppy disks to the list of prohibited personal devices. Noted policy on encryption of removable media when new information is being returned to a customer. Section 6.3.4 was updated to remove the reference that lists the Office of Systems Operations and Hardware Engineering (OSOHE) as the central tracking office for public key certificates.				
4.2	09/16/2016	Updated Section 2.1.4 by adding instructions for accessing the new (b) (7)(E) Furthermore, timeframes for certifying the (b) (7)(E) which replaced the (b) (7)(E) are included. Updated Section 5.3.1.9 to match because Sections were identical.	(b) (6)	09/15/2016	(b) (6)	09/16/2016

4.3	09/22/2016	Section 6.3.1 Background was updated to not that authorized technical support personnel are permitted to use unencrypted removal media for hardware and software administration and technical support activities without SSA DC approval. FIPS 140-2 reference to NIST's Cryptographic Module Validation Program was also added.	(b) (6)	09/22/2016	(b) (6)	09/22/2016
4.4	9/26/2016	Updates to section 1 through section 7 to correct all maintenance findings noted during the annual review of the ISP. Additional updates based on the ISP annual review are undergoing research and review and will be incorporated in later revision of the ISP. This constitutes the annual review of the ISP.	(b) (6)	09/29/2016	(b) (6) t	09/30/2016
4.5	10/14/2016	Enhancements made to section 1.7 to clarify the agency's requirements for training as well as the timeframes for training completion	(b) (6)	09/26/16	(b) (6)	10/14/2016
4.6	01/24/2017	Updates to section 1.5.2.8 to better define responsibilities for the sharing of information, such as code, on public sites. Corrected Security Authorization Process for External Systems document link in sections 3.6.2.2 and 3.7.1.	(b) (6)	01/19/2017	(b) (6)	01/24/2017
4.7	02/03/2017	Updates to sections 3.1.5 and 3.1.6 to remove "(b) (7)(E) and clearly identify allowed Web Conferencing and Instant Messaging solutions.	(b) (6)	02/03/2017	(b) (6)	02/03/2017
4.8	02/10/2017	Removed link to OIG/Office of Investigations (OI) in section 5.3.1.2. Updated section 3.6.2.2 with minor word changes to read more clearly.	(b) (6)	02/10/2017	(b) (6)	02/10/2017

4.9	02/22/2017	Updated term “individuals with significant information security responsibilities” to “personnel performing roles with significant cybersecurity responsibilities” in Section 1.7.	(b) (6)	02/22/2017	(b) (6)	02/22/2017
5.0	03/16/2017	Updates to Section 7.1 to establish that a risk-based determination is made after a waiver request is submitted. Reference to OPM CFR Part 930.301 removed from Section 1.7	(b) (6)	03/16/2017	(b) (6)	03/16/2017
5.1	03/22/2017	Replaced the broken IT Inventory Maintenance Procedures and Current Agency IT Inventory links with the updated link to the Enterprise Architecture (EA) Inventory Policy in Section 4.1.1. Updated Section 4.4.1 with minor word changes to read more clearly. Modified Section 5.3.1.8 by inserting the word, “performing”, in the (b) (7)(E) description.	(b) (6)	03/22/2017	(b) (6)	03/22/2017
5.2	04/12/2017	Added the word, “immediately”, to the reporting requirements for Phishing attacks in Section 5.2.1.1 to allow for consistency with requirements for general intrusion and Vishing attacks, as well as consistency with user training material	(b) (6)	4/11/2017	(b) (6)	4/12/2017
5.3	04/21/2017	Updated reference to Division of Compliance and Oversight (DCOver) to Division of Compliance and Assessments (DCA) in Section 1.4, per the 2017 Office of Information Security (OIS) Realignment. Replaced the following broken links: (b) (7)(E) in Sections 2.1.4 and Section 5.3.1.9; Risk Acceptance Handbook in Section 3.6.2.2; and Security Configuration Guides in Section 3.1.4.	(b) (6)	4/21/2017	(b) (6)	4/21/2017

5.4	05/02/2017	Modified statement in Section 3.4.2 to require authorized security configuration standards for authorized platforms and solution architectures. Also, included the requirement that security configuration standards be reviewed annually.	(b) (6)	05/02/2017	(b) (6)	05/02/2017
5.5	05/04/2017	Inserted a new sub-section into Section 4 to implement an event logging policy and define logging requirements. Renumbered Section 4 in order to insert new sub-section as 4.1.	(b) (6)	05/02/2017	(b) (6)	05/04/2017
5.6	05/09/2017	Updated links to revised ISO Manual in Sections 2.1.1.1, 2.1.1.2, 2.1.1.3, 2.1.1.5, 2.1.4, and 5.3.1.9. Replaced the broken External Service Provider links in Section 4.6.2.4.	(b) (6)	05/09/2017	(b) (6)	05/09/2017
5.7	05/17/2017	Simplified the Incident Reporting Process in Section 5.2.1.1 to eliminate the requirement to report to a manager and require all incidents be reported to ^SOC. Directed customers to the Social Engineering Resources webpage for more information.	(b) (6)	05/17/2017	(b) (6)	05/17/2017
5.8	05/24/2017	Updated links to the Mandatory Information Security Awareness Training webpage, Cybersecurity Communication & Training Portal, Role-Based Cybersecurity Training Portal, and Training Evidence Collection Form in Section 1.7. Updated link and name for OPE's Center for Suitability and Personnel Security (CSPS), as well as minor re-wording in Section 1.8.1. Updated link to Secure Partners List in Sections 6.4.1 and 6.4.2.	(b) (6)	05/24/2017	(b) (6)	05/24/2017
5.9	05/30/2017	Modified Sections 6.4.1 and 6.4.2 with minor wording changes and reformatting for clarity and consistency.	(b) (6)	05/25/2017	(b) (6)	05/30/2017

6.0	06/06/2017	Removed a paragraph from the Credential Management Policy in Section 2.1.1.3 and inserted it in the Web Services Security Policy in Section 3.5.1, as it is more applicable to Web Services Security. Modified Section 5 by removing a redundant paragraph from the Contingency Planning and Incident Response Introduction. Similar paragraph remains present in Section 5.2.1.1.	(b) (6)	06/05/2017	(b) (6)	06/06/2017

TABLE OF CONTENTS

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 Management Act (FISMA) of 2002 (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.

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.

1.2 Statutory Requirements

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) 144, 199, 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.

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.

1.3 Definitions

Policy – A high-level statement 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.

1.4 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:

- Office of Information Security (OIS)
- Office of Systems (OS)
- Division of Compliance and Assessments (DCA)
- Office of Public Service and Operations Support (OPSOS)
- Regional Center Directors for Security and Integrity (CDSI)
- Office of Systems Operations and Hardware Engineering (OSOHE)
- Division of Information Systems Security (DISSAO)
- Division of Systems Security and Program Integrity (DSSPI)
- Office of Disability Adjudication and Review (ODAR)

- Office of General Counsel (OGC)
- Office of the Inspector General (OIG)
- Office of Budget, Finance, Quality, and Management (DCBFQM)
- Other decentralized components (see Figure 1 below)

.

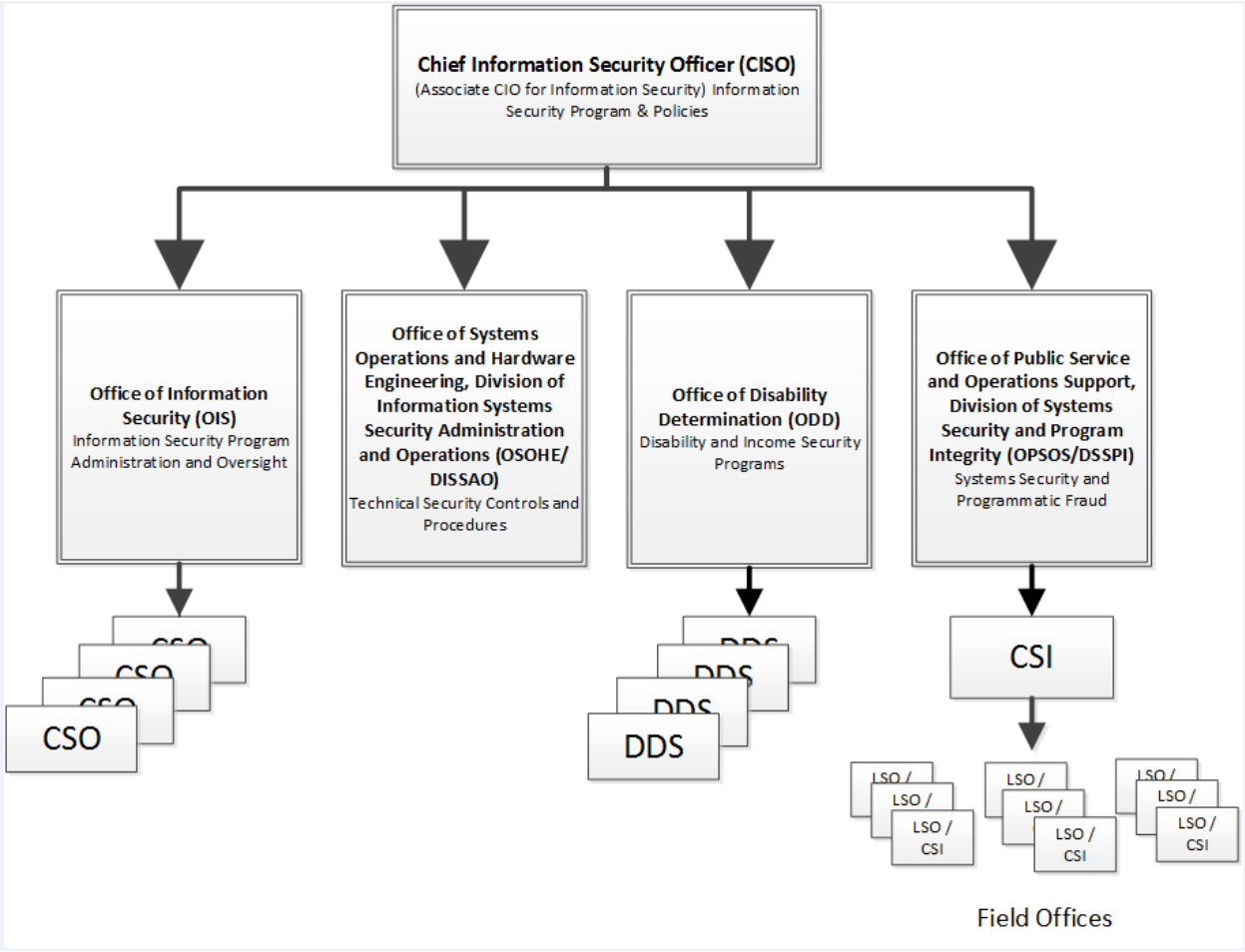

Figure 1. Security Organizational Structure

Laws and Regulations

The CISO is SSA's Senior Agency Information Security Officer (SAISO). The SAISO delegates FISMA IT security program functions to the systems, operations, business functions directorates, and components. These organizations are responsible for ensuring compliance with:

- FISMA,
- OMB,

- Federal Standards,
- SSA IT security policies and standards
- Keeping OIS advised of all IT security activities, issues, and accomplishments.

OIS is charged with security oversight, policy, and training for SSA's Information Security Program. DISSAO is responsible for technical security controls and procedures. DSSPI, CDSI, ODAR, DCBFQM, OGC, and OIG are responsible for coordinating all security activity in their respective areas. They are in charge of implementing National and Regional security directives and enforcing compliance. DSSPI and CDSI work with Local Security Officers (LSOs) at the field office level for issues involving Information Security.

Within SSA's Headquarters Central Office, Component Security Officers (CSOs) are responsible for ensuring compliance within their respective headquarters components. ODD in Office of Operations coordinates DDS operations, and distributes additional agency policy transmittals specific to the DDSs.

Regulation No. 1 and the Social Security Act

The Social Security Board, in 1937, established Regulation No. 1. This document guarantees the privacy and confidentiality of all information submitted to SSA. The regulation ensures the confidentiality of records furnished by employees, employers, and citizens so they are not reluctant to submit complete and accurate information.

In 1939, **Section 1106** of the Social Security Act was enacted and became the statutory basis for maintaining the confidentiality of SSA information. This section states that no file, record, report, paper, or other information obtained at any time from any person may be disclosed except as provided by regulations from SSA or other applicable laws. These actions indicated the high regard that the founders of SSA had for the protection of personal information.

Executive Order 10450 (1953)

Executive Order 10450, Security Requirements for Government Employment (April 27 1953), 18 FR 2489, as amended, establishes security requirements for government employment. It provides for an investigation of employees of the Federal government. It also provides for the scope of the investigation based on the sensitivity / risk of the position occupied.

FOIA (1966)

FOIA, Public Law (P.L.) 93-502, was passed by Congress in 1966. It opened the workings of the government to the public eye. Under this Act, and substantial amendments passed in 1974, the public is able to request and receive administrative and instructional material as well as personal information that does not clearly constitute an unwarranted invasion of an individual's personal privacy. The SSA Freedom of Information Officer (FOIO) and staff are available to resolve questions concerning FOIA.

Privacy Act (1974)

The Privacy Act, P.L. 93-579, was passed in 1974 in reaction to the proliferation of records maintained by Federal agencies on individuals. It required agencies to identify systems of records, which they maintained on the public and their employees. These systems of record published in the Federal Register are to provide a public record of the information maintained on private individuals and employees.

This legislation is deliberately restricted to Federal agencies. They did not include private institutions, as they did not want it to appear that the government was creating or enabling the creation of a national database with personal information on all citizens.

Agencies are required to maintain the data received from individuals and employees without alteration or addition. Disclosure to persons or other agencies was allowed only by consent of the individual. Exceptions, not requiring consent to disclose, included a specific listing of "routine uses". These were either necessary and beneficial to the individual or employee, or beneficial to all in reducing administrative costs, fraudulent payments, or benefits.

An example of a "routine use" would be sharing information on an SSA claim for benefits with the Railroad Board to determine jurisdiction. Another common "routine use" is the sharing of SSA benefit information on claimants to determine or establish entitlement to state public aid benefits.

This legislation not only required agencies to maintain the confidentiality of information collected on individuals and employees, but to also disclose publicly what they maintained and how the data was to be utilized. The SSA Privacy Officer and staff are available to resolve questions concerning the provisions of this Act.

Tax Reform Act (TRA) (1976)

The TRA of 1976, Public Law 94-455, affects SSA's use of earnings data provided by the IRS. The tax returns information can be used by SSA only to administer the parts of the Social Security Act for which SSA has responsibility. It is illegal to disclose earnings data unless specifically permitted under the Internal Revenue Code.

Thus, the TRA imposes additional requirements for the protection of IRS data furnished to SSA. As a result, additional safeguards are sometimes necessary when SSA is doing a project involving IRS data.

Sunshine Act (1977)

The Sunshine Act, effective in 1977, amended the FOIA. The Social Security Act no longer qualifies as a statute cited as a legal basis for denying FOIA requests. Based on this amendment, SSA is required to disclose any information requested, with some exceptions. The burden is consigned to SSA to support withholding, rather than on the requester to justify disclosure.

Upon request, SSA is required to disclose all operating instructions, policies, memoranda, papers and documents. The only exceptions are those, which are specifically restricted because their disclosure could produce harm to the programs that SSA administers.

Internal Revenue Code (IRC) (1986)

SSA obtains, processes, and stores income tax return information provided through agreements with the IRS. In order to properly safeguard this data, SSA complies with requirements spelled out in the IRC Sections 6103(p), 7213(a), and IRS 1075.

Section 6103(p) defines the conditions under which IRS income tax data must be safeguarded, and under what conditions it may be further disclosed.

Section 7213(a) describes the awareness and training requirements for compliance with the IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) program as well as defining the penalties for browsing or otherwise disclosing tax return information.

Federal Managers' Financial Integrity Act (FMFIA) of 1982

The FMFIA, enacted in 1982, requires agencies to report on the status of their management control systems. It also requires that the OMB establish guidelines for the evaluation, by agencies, of their systems of internal accounting and administrative control to determine whether such systems meet requirements, which ensure:

- Obligations and costs are in compliance with applicable law;
- Funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation;
- Revenues and expenditures applicable to agency operations are properly recorded and accounted for; permit the preparation of accounts and reliable financial and statistical reports; and maintain accountability over the assets, and
- Programs are effectively carried out in accordance with applicable law and management policy.

The FMFIA further requires the U.S. General Accountability Office (GAO) to prescribe standards upon which to base the level of achievement of the above requirements. Finally, the law requires the head of each executive agency to annually prepare and submit a statement to the President and Congress as to whether the agency's systems of internal accounting and administrative control fully comply with the requirements listed above.

SSA has actively pursued the Act's goals since its passage. SSA is segmented into management control areas covering field offices, processing centers, data operations centers, financial management systems, and other central office activities. Reviews of these areas identify management control weaknesses to ensure corrective action.

Every year the Commissioner reports on the adequacy of SSA's management control system. This report is consolidated with those of other Federal agencies and transmitted to the President and Congress.

Counterfeit Access Device and Computer Fraud and Abuse Act of 1984

This act, Public Law 98-473, Title II, and Chapter XXI prohibits knowingly accessing any computer without authorization, or exceeding authorization to obtain information covered by any privacy regulation, financial information regulation, non-disclosure regulation, or national security reasons.

Computer Fraud and Abuse Act (CFAA) of 1986

The CFFA, Public Law (P.L.) 99-474, prohibits unauthorized access of any U.S. Government department or agency computer, or exceeding authorized access to these computers, to conduct fraud, or alter, damage, or destroy any information contained therein. While the CFAA appears to parallel the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, it is more specifically targeted to U.S. Government computer systems and covers a broader range of data access.

Computer Security Act (CSA) of 1987

The CSA of 1987, Public Law 100-235, and the CSA Amendments of 1992, establish the National Institute of Standards and Technology (NIST) as the agency responsible for developing standards and guidelines needed to ensure the cost-effective security and privacy of sensitive information in unclassified Federal computer systems.

The CSA also requires that each Federal agency must provide mandatory, periodic training in computer security awareness, and accepted security practices, for all employees involved with the management, use, or operation of each Federal computer within the agency.

Government Information Security Reform Act (GISRA)

The GISRA amends the Paperwork Reduction Act (PRA) of 1995 by enacting a new subchapter on "Information Security". The GISRA seeks to ensure proper management and security for the information resources supporting Federal operations and assets, and primarily addresses the program management, and evaluation aspects of security. It requires:

- Annual agency program reviews;
- Annual Inspector General (IG) evaluations;
- Agency reporting to OMB the results of IG evaluations for unclassified systems and audits of IG evaluations for national security programs; and
- An annual OMB report to Congress summarizing the materials received from agencies.

Agencies submit this information (beginning in 2001) as part of the budget process.

Computer Matching and Privacy Protection Act (CMPPA) of 1988

Computer matching is an effective strategy against fraud and abuse in government assistance programs. To ensure that Federal agencies use computer matching appropriately, the CMPPA, P.L. 100-503, passed in 1988. It requires agencies to give notice before taking action based on a match. Computer matching is the computerized comparison of records for the following purposes:

- Establishing or verifying eligibility for a Federal benefit program.
- Recouping payments or delinquent debts under such programs.

SSA Publication No. 30-011, SSA Matching Operations Inventory, contains the current list of SSA matches. These include internal SSA matches, matches with other agencies, states, and local governments. Each match project has a designated SSA match manager.

OMB Circular A-123 (Revised June 1995)

This circular supports the requirements set forth in the FMFIA regarding internal accounting and administrative control standards. The circular prescribes policies and procedures to be followed by agencies in establishing, maintaining, evaluating, improving, and reporting on internal controls within their program and administrative activities.

Federal Financial Management Improvement Act (FFMIA) of 1996

The FFMIA requires that agency financial management systems comply substantially with federal financial management systems requirements, or that a remediation plan be developed to bring the agency into compliance within three (3) years.

OMB Circular Appendix III A-130, Security of Federally Automated Information Resources (Revised February 1996)

This circular generally addresses the management of Federal information resources. However, Appendix III specifically identifies, and establishes a minimum set of controls to be included in Federal Automated Information Systems (AIS) security programs. It also establishes responsibility for the security of agency AIS programs, and requires that agencies establish a security awareness and training program to ensure that all managers and operators of Federal computers are aware of their responsibilities and know how to fulfill them.

Presidential Decision Directive-62 (PDD-62, 1998) "Combating Terrorism"

PPD-62 establishes the office of the National Coordinator for Security, Infrastructure, Protection and Counter-terrorism. This office provides oversight authority for policies and programs in areas such as critical infrastructure protection.

PDD-63 (1998) "Critical Infrastructure Protection"

PPD-63 calls for a national effort to ensure the security of interconnected U.S. Infrastructures. It requires that:

- The CIO is responsible for information Assurance.
- Each agency must:
    - Protect its own critical infrastructure,
    - Conduct vulnerability assessments,
    - Appoint a Chief Infrastructure Assurance Officer (CIAO), who is responsible for the protection of all other (non-Information Systems) aspects of critical infrastructure.

PDD-67 (1998) "Enduring Constitutional Government and Continuity of Government Operations"

PDD-67 directs that all agencies have a viable Continuity of Operations Plan (COOP) in place.

NIST Special Publication (SP) 800-18, Guide for Developing Security Plans for Information Technology Systems (1998)

SP 800-18 replaces OMB Bulletin No. 90-08, and provides guidance on security planning activities. Each agency must implement security plans for all systems that contain sensitive information, and must update these plans whenever a system is significantly modified. The publication also identifies the information and format for sensitive system plans including categories and controls.

Homeland Security Presidential Directive 12 (2004)

HSPD-12 is a presidential directive that requires the establishment of a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal government to its employees and contractors. The directive sets out to eliminate the wide variations in the quality and security of forms of identification used to gain access to Federal facilities and IT networks. The primary goals of HSPD-12 are to enhance security by verifying the identity of individuals, to increase government efficiency, to reduce identity fraud, and to protect personal privacy.

NIST established standards for agencies (FIPS 201-1) and selected the Personal Identity Verification (PIV) smart card as the Federal credential. Further direction is provided by the Federal CIO Council in the form of the "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance", Version 2.0.

OMB Circular A-127 (Revised January 2009)

This circular prescribes policies and procedures to be followed by agencies in developing, operating, evaluating, and reporting on financial management systems. This circular also

supports the FMFIA and the Budget and Accounting Procedures Act (BAPA) of 1950, as does OMB Circular A-123, but focuses specifically on financial management systems.

OMB Memorandum (M) 11-11 (2011)

Released on February 3, 2011, OMB M-11-11 provides requirements and deadlines for drafting and issuing an implementation policy for the use of PIV smart card as the common means for accessing Federal facilities, networks, and Information Systems. All Federal agencies must develop and issue this implementation policy by March 31, 2011, and the following requirements must be included:

- Effective immediately, prior to being operational, all new systems under development must enable the use of PIV credentials in accordance with NIST guidelines.
- Effective the beginning of FY2012, existing physical and logical access control systems must upgrade to use PIV credentials in accordance with NIST guidelines, prior to the agency using development and technology refresh funds to complete other activities.
- Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and the Federal Acquisition Regulation (FAR). In order to ensure government-wide interoperability, OMB M-06-18, "Acquisition of Products and Services for Implementation of HSPD-12" requires agencies to acquire products and services approved as compliant with Federal policy, standards and supporting technical specifications.
- Agency processes must accept and electronically verify PIV credentials issued by other Federal agencies.
- The government-wide architecture and completion of agency transition plans must align as described in the Federal CIO Council's "Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance".

1.5 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.).

1.5.1 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 1.7 Information Security Training and Awareness Policy).
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).

1.5.2 User Responsibilities

1.5.2.1 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 2.1 Information Systems Logical Access Control Policy.
- Be accountable for all transactions issued in connection with their Personal Identification Number (PIN) / Identification (ID).
- 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.

1.5.2.2 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.

1.5.2.3 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.

1.5.2.4 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 1.7 Information Security and Awareness Policy).
- Participate in all required Information Security training and awareness (ISP 1.7 Information Security and Awareness Policy) activities as identified by management or required by policy.

1.5.2.5 Personally Identifiable Information (PII)

- Agree to follow the guidance in the Administrative Instructions Manual System, General Administration Manual, Chapter 15, PII Loss and Remediation regarding PII.
- Protect PII whether officially on duty or not on duty, at their official duty station, another official work location, or an alternate duty station, by following the "What You Need to Know About PII" handbook.
- Report any suspected breaches of PII using the PII Reporting Tool.

1.5.2.6 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 3.4 Hardware, Software, and Platform Configuration) 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 unless otherwise authorized by management.
- 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 ISP 6.4Section I: Overview of Information Security, as well as other forms of electronic communications.
- Properly safeguard removable media.

1.5.2.7 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.
- Safeguard and properly dispose of any other sensitive printed material.

1.5.2.8 Public Disclosure

- Employees must follow the SSA's Social Media Policy when using social media web sites for both official business and personal use.
- 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.

1.5.2.9 Incident Reporting

- Report suspected virus attacks, malicious / unauthorized intrusion or access in accordance with (ISP 5.2 Security Incident Identification, Reporting and Resolution) Security Incident Identification, Reporting, and Resolution.
- 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 5.3 Criminal Violations and Fraud) Policy Violations Reporting Process & Security Administration Reports.

1.5.3 Consequences of Rules Violations

- In those instances where users do not follow the prescribed rules of behavior, there are penalties enforceable under existing policy and regulations ranging from official written reprimands through suspension of system privileges, temporary suspension from duty,

removal from current position, to termination of employment, and possibly criminal prosecution.

- Users who fail to adequately safeguard PII or who violate agency policies for safeguarding PII may be subject to disciplinary action, up to and including removal from Federal service or other actions in accordance with applicable law and agency policy.
- Supervisors should understand that they also might be subject to disciplinary action for their failure to take appropriate action upon discovering a breach, or their failure to take required steps to prevent a breach from occurring, including adequately instructing, training, and supervising employees regarding their responsibilities for safeguarding PII.
- The Agency Policy for Systems Access, Table of Penalties for Violations and Acknowledgements Statement by Employee provides further information. Additional information can be located in the Code of Federal Regulations.

1.6 Limited Personal Use of Government Office Equipment, including IT

The policy on the personal use of Government equipment is an SSA official document and is located at SSA policy for personal use of government equipment.

1.7 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.

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, *A Role-Based Model for Federal Information Technology/Cybersecurity Training.*

1.7.1 Annual Information Security Awareness Training

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

1.7.2 Role-based Training for Personnel Performing Roles With Significant Cybersecurity Responsibilities

The following requirements must be met:

- All SSA and DDS employees identified as personnel performing roles with significant cybersecurity responsibilities must complete 8 hours of role-based cybersecurity training, in addition to information security awareness training, each Fiscal Year.
- Please visit the Role-Based Cybersecurity Training Portal for criteria the agency uses to identify roles and personnel performing significant cybersecurity responsibilities, specific employee and contractor training requirements, and available training resources.
- Contract vendors must ensure personnel complete role-based information security training each Fiscal Year in order to maintain personnel skillsets commensurate with information security job functions necessary for contract fulfillment.

1.7.3 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.

1.7.4 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.
- SSA and DDS employees identified as personnel performing roles with significant cybersecurity responsibilities must upload completed role-based cybersecurity training evidence using the Training Evidence Collection Form.

1.8 Personnel Security and Suitability Program

1.8.1 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.

1.8.2 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.
- 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.

1.8.3 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 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.

1.9 References

1.9.1 Laws, Regulations, and Guidance

E-Government Act of 2002, P.L. 107-347, Title III, Federal Information Security Management Act (FISMA) (2002)

1.9.2 OMB

OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources

1.9.3 Office of Personnel Management

OPM 5 CFR, Subpart C, Part 930.301, *Information Security Responsibilities for Employees who Manage or Use Information Systems*

1.9.4 NIST

- Special Publication 800-16, *Information Technology Security Training Requirements: A Role and Performance-Based Model*
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*

1.9.5 National Archives and Records Administration (NARA)

- Records Management by Federal Agencies
- http://www.archives.gov/records-mgmt/grs/grs20.html - electronic records
- http://www.archives.gov/records-mgmt/grs/grs07.html - financial records

- http://www.archives.gov/records-mgmt/grs/grs03-2.pdf- reference to Information system security records.
- http://www.archives.gov/records-mgmt/grs/grs24.html - references PKI records and 7 years

2 Section II: Access Control

Introduction: The Information Security Policy (ISP), along with other supporting standards and procedures, establishes the basis for implementing secure logical access controls for the Social Security Administration's (SSA) Information Technology (IT) resources and associated Information Systems.

Purpose: This section provides Information Security policy and suitability requirements for individuals with access to SSA Information Systems and Automated Information Systems (AISs). SSA's policy for SSA's Personnel Security and Suitability Program for Information Systems-related positions is part of the overall Agency Information System's Security Program.

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 to 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.

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

2.1 Information Systems Logical Access Control Policy

2.1.1 Background

SSA's logical access control policy conforms to Federal regulations and standards. SSA's logical access policy complies with the Federal Information Security Management Act of 2002 (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).

2.1.1.1 General

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., Second UserID, Time Sharing Option (TSO) and Customer Information Control System (CICS), passwords, and profiles) for SSA's

computing environments, and computing platforms, such as Mainframe Windows, and UNIX.
- The Information Security Officer (ISO) Manual contains additional actions for Security Officers to perform their responsibilities related to access control management.

2.1.1.2 Identity Management

A digital identity permits access to SSA's Information Systems found in the following locations:

- 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.

2.1.1.3 Credential Management

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

- All SSA Information Systems must uniquely identify, and authenticate all user credentials when presented to an Information System.
- The Electronic Personal Enrollment Credential System (EPECS) enrollment process begins the initial Information System access process, and results in the creation of the user's unique identity.
- EPECS enrollment automatically generates the new user's TOP SECRET Personal Identification Number (PIN); it does not grant systems access.
- The authorized manager must submit a request for access to SSA Systems to assign a base profile; this releases the PIN from the TOP SECRET hold zone, enabling system access.

    - 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.

- SSA Employees must use their agency issued HSPD-12 PIV cards for all (i.e., Windows environments) logical access to agency computers.
- 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:

  - Be submitted upon notification of an employee or contractor separating from SSA.
  - If emergency termination is required, requests must be expedited by Managers for immediate removal.
  - Within 18 hours of notification, Managers must confirm all accounts have been disabled or removed. For information regarding the process for removing employee and contractor PIV access, see AIMS MRM 04.51 Personal Identity Verification and Credential Issuance Process and Section 3.6 of the ISO Manual.

- (b) (7)(E) [redacted]).
- Managers must deactivate systems access for employees on extended leave (greater than 74 days).
- Temporary Access Accounts (i.e., contractors, auditors, student volunteers, host enrollees, etc.) have specific requirements.

  - Third parties or business partners must adhere to SSA-approved access processes when granted access to SSA Information Systems.
  - If contractors, student volunteers, or host enrollees are allowed temporary access to SSA systems, such access is limited to one (1) year or for the contract period, whichever is less.
  - Contract personnel requiring systems access beyond one (1) year must submit a new request for systems access annually.
  - Contractors and non-employees access to SSA Information Systems is restricted based on user need-to-know and must be required to perform official job duties.

- Service Accounts (sometimes referred to as machine or equipment PINs) are established only for a device, application, or other "non-person entity" that requires a PIN to execute a process, or access other devices and applications. For more information see the Account Type Matrix.

  - Service Accounts are special-purpose PINs approved for use in SSA operations, and are site-specific.

- Service accounts must be used only for running applications or scripts, and must be executed by the system.
- Windows service accounts must be placed in the designated service account Active Directory group. Please refer to the Account Type Matrix table for specific requirements.
- Service accounts can only be used for the actions approved in the original account request.
- To request a service account or change access for an existing service account, complete form SSA-1121. For service account procedures, see ISO Manual Section 3.1.1.

2.1.1.4 Credential and Password Policies

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

- System Users:
  - Must change their provided password to a unique password in cases of first-time access and password reset.
  - Never display, store, or place passwords in a commonly accessible location.
  - Never share or reveal passwords with anyone.
  - Never share HSPD-12 credentials (PIV smart cards).
  - Never allow others to use their workstations while logged on with the system user's credentials; this standard excludes authorized SSA technical support employees or contractors requiring troubleshooting issues (as they may need to perform work under a user's PIN.
- Managers, System Administrators, and authorized users must:
  - Change vendor-supplied default passwords for software, applications, and devices before the IT resource is utilized on SSA systems.
  - Configure system platforms to enforce password change rules.
  - Encrypt files that contain passwords.
  - Never store passwords in readable form, in batch files, automatic log-on scripts, software macros, terminal function keys, dial-up communications programs, or other locations.
- Privileged Users:
  - Account Administrators require a higher level of protection; they must use a password that includes upper / lower case, alphanumeric, and special characters.
  - Privileged users must use their standard account for all activities unless elevated privileges are needed.

- Privileged access rights must be removed when an account is disabled.
- Access rights must be removed whenever the account holder has a role change.
- Active Directory Enterprise and Domain administrator accounts must not have access to the internet.

2.1.1.5 Access Management

Once an identity is authenticated, a credential is issued, and procedures to create, manage, and delete privileges are established, the following applies:

- 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).

- Information System Managers (ISMs) 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.
  - ISMs 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).

- 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.
- Prior to the system sign-on process, a system notification banner must display information to the user stating users are accessing a U.S. Government Information System, appropriate authorized system use, privacy expectations, disciplinary actions,

and civil or criminal prosecution for unauthorized attempts to access or modify any part of SSA's systems.

- Account usage must be monitored, and user accounts must be reviewed periodically to ensure access is appropriate for each user's assigned duties; frequency of review depends upon account type (Information Security Officer (ISO) Manual, Sec. 3, "Access Control Administration", and Sec. 4 "Security Policy Implementation"):

    - All SSA Employees review triennially.
    - Contractors, temporary employees, Second UserIDs and new hire employees out-of band from triennial review annually.

- Second UserID: To comply with the agency policy of Least Privilege, and Need-to-Know, SSA established the Second UserID process:

    - A Second UserID, different from, but linked to, the Primary ID is issued; technical personnel (e.g., developers) use the Second UserID to access production resources.
    - Authorized personnel monitor the Second UserID activity performed on production resources.
    - Procedures for monitoring and audit information for the Second UserID 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.

2.1.2 Authorities

- Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53)
- OMB Circulars and Memoranda
- Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance December 2011, and
- Applicable NIST and SSA guidance is provided.

2.1.3 Definitions

Defined terms specific to this section:

- **Access Control** – The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter

specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances) (source: Committee on National Security Systems Instruction (CNSSI) 4009).

- **Access Control List(s) -** A register of users (including groups, machines, and processes) who have been given permission to use a particular system resource, and 2) the types of access they have been permitted (source: NIST SP 800-12). Also see CNSSI-4009.
- **Account Management, User** – involves the process of requesting, establishing, issuing, and closing user accounts; tracking users and their respective access authorizations; and managing these functions (source: NIST SP 800-12).
- **Access Profile** – Association of a user with a list of protected objects that the user may access (source: CNSSI-4009).
- **Access Type** – Privilege to perform action on an object; read, write, execute, append, modify, delete, and create are examples (source: CNSSI-4009).
- **Authentication** – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an Information System (source: Federal Information Processing Standard (FIPS) 200)
- **Authenticity** – The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, message, or message originator (source: NIST SP 800-53).
- **Authorization** – Access privileges granted to a user, program, or process; or the act of granting those privileges (source: CNSSI-4009).
- **Credential** – Evidence or testimonials that support a claim of identity or assertion of an attribute, and usually are intended to be used more than once (source: CNSSI-4009).
- **Digital Identity** – Identity, Credential, and & Access Management (ICAM) Services Framework service type made up of service component:

    - The representation of Identity in a digital environment;
    - The digital identity can also be associated with a credential for enabling various levels of identity authentication as the basis for authorizing access to applications and facilities (source: FICAM Roadmap and Implementation Guidance).

- **Identity** – The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity (source: FICAM Roadmap and Implementation Guidance).
- **IT resources –** Systems (including programmatic, administrative, and support systems necessary to accomplish SSA's mission), databases, data, hardware, software, and the platforms on which they reside.
- **Least Privilege -** The security objective of granting users only those accesses they need to perform their official duties (source: NIST SP 800-12; also see CNSSI-4009).
- **Logical Access** – Computer-based access controls can prescribe not only who or what (e.g. In the case of a process) is to have access to a specific system resource, but also the permitting type of access (source: NIST SP 800-12).

- **Need-to-Know** – A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more.
- **Non-Person Entity** – Infrastructure components (e.g., workstations, servers, firewalls, routers, batch process machine to machine communication) with the authority to perform operations on behalf, and under the awareness of a Person (human) Entity, who is responsible for the authority to perform the operation.
- **Object** – Passive Information System-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object implies access to the information it contains (source: CNSSI-4009).
- **PIN -** An alphanumeric code or password used to authenticate an identity (source: FIPS 140-2; also see NIST SP 800-63, CNSSI-4009 and FIPS 201-2).
- **Privileged User** – One who is authorized (and therefore trusted) to perform security-relevant functions that ordinary users are not authorized to perform (source: CNSSI-4009, NIST SP 800-53).
- Separation of duties:
    - A basic internal control that prevents or detects errors and irregularities by assigning the responsibility for initiating and recording transactions and for the custody of assets to separate individuals (source: ISACA).
    - The organization:
        - Separates (Assignment: organization-defined duties of individuals);
        - Documents separation of duties of individuals; and
        - Defines Information System access authorizations to support separation of duties (source: NIST SP 800-53).
    - Dividing roles and responsibilities so that a single individual cannot subvert a critical process (e.g., in financial systems, no single individual should normally be given authority to issue checks. Rather, one person initiates a request for a payment and another authorizes that same payment (source: NIST SP 800-14).
    - Organizations should strive for separation of duties between security personnel who administer the access control function and those who administer the audit trail (source: NIST SP 800-14).
- **System Managers** – Responsible for the physical and electronic security of the data and the data processing capabilities of their AIS(s).
    - Generally, this is the management official for the staff that is operating and maintaining the system.
    - Systems Managers may be office Managers, Security Officers, or employees designated by management.
- **Unauthorized Access -** Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use (source: FIPS 191 and CNSSI-4009).

2.1.4 Security Administration Reports

(b) (7)(E)

- (b) (7)(E)

2.2 Systems Access Security Administration Software

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., establishing PINs, individual accountability, suspensions, and reinstatements) and performing other security actions and incidents (e.g., logging / audit features, etc.). Users' system activity must be traceable to specific user accounts and must be logged and audited (ISP 4.4.2 Audit Requirements and Guidelines)
- Have encryption capability.
- Have reporting capability.
- Local application PINs access must be appropriate and deleted if no longer required.

2.3 Personnel Security

SSA's Information Systems security policy for SSA's Personnel Security and Suitability Program for AIS-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.

2.4 Roles and Responsibilities

The following components or groups have specific responsibilities.

- The Office of Information Security (OIS) must:
    - Provide criteria determining the frequency of access control reviews.
    - Be responsible for policy and oversight.
    - Approve all standards and procedures for logical system access.

- The Contracting Officer's Representative (COR) or their designees must work with managers to ensure contractor access is required for official contractual duties:
    - See the Contracting Officer Technical Representative web page.
    - See Administrative Instruction Manual Systems (AIMS) Chapter 6, Instruction #5.
- Information Security Officers (ISOs) must 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.
- Managers or their designees must:
    - (b) (7)(E) [redacted]
- Network Administrative staff (e.g., Site LAN Coordinator (SLC) / LAN Administrator, etc., under the direction of the local manager, and often working in conjunction with OSOHE, must:
    - Monitor user accounts and activity to ensure access to the network is appropriately limited and consistent with business needs defined by management.
    - Implement LAN security standards at the local site.
    - Ensure 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.

- Ensure all LAN configurations uniquely identify and authenticate all user credentials when presented to an Information System.
- Ensure 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).
- Report incidents to the National Network Service Center (NNSC) and notify their CDSI / CSO.

2.5 References

2.5.1 Office of the President

- Executive Order 10450 – Security Requirements for Government Employees (1953)
- Executive Order 12968 – Access to Classified Information (1995)

2.5.2 OMB

- Circular A-123, Management's Responsibility for Internal Control
- Circular A-130, Management of Federal Information Resources
- Memorandum (M) 06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
- M-06-06, Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12 (February 17, 2006)
- M-06-16, Protection of Sensitive Agency Information, June 23, 2006
- M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
- M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005
- M-08-01, HSPD-12 Implementation Status (October 23, 2007)
- M-11-11, Continued Implementation of HSPD 12 – Policy for a Common Identification Standard for Federal Employees and Contractors
- Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011

2.5.3 NIST

- FIPS 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, June 23, 2006
- FIPS 199, Standards for the Security Categorization of Federal Information and Information Systems, February 2004
- FIPS 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors, August, 2013

- SP 800-12, An Introduction to Computer Security: The NIST Handbook – Chapter 10, October 1995
- SP 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010
- SP 800-39, Managing Information Security Risk: Organization, Mission, and Information View, March 2011
- SP 800-53, Recommended Security Controls for Federal Information and Information Systems
- SP 800-60 Volume I, Revision 1, Guide for Mapping Types Information and Information Systems to Security Categories, August 2008
- SP 800-60 Volume II, Revision 1, Appendices to Guide for Mapping Types Information and Information Systems to Security Categories, August 2008
- SP 800-63-1, Electronic Authentication Guideline, December 2011
- SP 800-73-3, Interfaces for Personal Identity Verification – Part 1: End-Point PIV Card Application Namespace, Data Model and Representation, February 2010
- SP 800-73-3, Interfaces for Personal Identity Verification – Part 2: End-Point PIV Card Application Command Interface, February 2010
- SP 800-73-3, Interfaces for Personal Identity Verification – Part 3: End-Point PIV Client Application Programming Interface, February 2010
- SP 800-73-3, Interfaces for Personal Identity Verification – Part 4: The PIV Transitional Interfaces and Data Model Specification, February 2010
- SP 800-76-2, Biometric Data Specification for Personal Identity Verification, July 2013
- SP 800-78-3, Cryptographic Algorithms and Key Sizes for Personal Identity Verification, December 2010
- SP 800-100, Information Security Handbook: A Guide for Managers, October 2006
- SP 800-12, An Introduction to Computer Security: The NIST Handbook – Chapter 10, October 1995

2.5.4 SSA

- Account Type Matrix
- Physical Access Management (PAM)
- Office of Personnel–Center for Security and Suitability Program
- Information Security Officer (ISO) Manual
- Personal Identity Verification and Credential Issuance Process
- SSA Mainframe Administration Standards, September 30, 2011
- SSA Profile Naming Standard
- Automated Systems Access Forms Environment (ATSAFE) Procedures; Office of Systems Operations and Hardware Engineering
- Systems Sanctions Violations - Agency Policy and Acknowledgement Statement
- Systems Access Management Portal (SAM)
- Triennial Certification (TEC)

2.5.5 U.S. Department of Homeland Security (DHS)

HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004

2.5.5.1 Laws and Regulations

- FISMA of 2002
- The Privacy Act of 1974, Public Law (P.L.) 93-579, 5 United States Code (USC) 552a
- Government Information Security Reform Act (GISRA), P.L. 106-398, Title X (2000)
- Code of Federal Regulations (CFR), Title 5 - Administrative Personnel:
    - Part 731, "Suitability",
    - Part 732, "National Security Positions",
    - Part 736, "Personnel Investigations".
- The Privacy Act of 1974, P.L. 93-579, 5 U.S.C. 552a
- Civil Service Reform Act of 1978, 5 U.S.C. 3111, Section 301(a)
- FISMA of 2002

3 Section III: Network Protection

Introduction: This section establishes SSA security policies, Federal regulations, and business requirements for wireless, web services, and cloud computing technology in order to protect the network. SSA's policy for network protection is to ensure the confidentiality, integrity, and availability for collecting, disseminating, and transmitting SSA sensitive information, including record information protected under the Privacy Act of 1974, and Section 1106 of the Social Security Act.

Purpose: This section consists of the provisions and policies adopted by SSA's network administrator(s) to prevent and monitor unauthorized access, misuse, modification, or denial of a computer, network and network-accessible resources.

SSA's Network Protection policy involves the authorization of access to data in a network, controlled by the local SSA network administrator(s). It covers a variety of SSA computer networks, both public and private. It also covers all communication technology devices connected to SSA's internal networks, including wired, wireless, World Wide Web, and cloud technologies. Cloud computing is a model for delivering computing services that is characterized by the ability to provide on-demand network access to shared computing resources, (e.g., networks, servers, storage, and applications) that can be rapidly provisioned. The National Institute of Standards & Technology (NIST) has defined five (5) essential characteristics of cloud computing: on-demand service, broad network access, resource pooling, rapid elasticity, and measured service. This section establishes agency security policy in support of the Chief Information Office (CIO) Cloud Computing Policy.

SSA's network protection policy safeguards the network, as well as protecting and overseeing operations being performed.

Scope: This policy applies to all SSA employees, Disability Determination Services (DDS) employees, temporary staff, contractors, and other users when they act on behalf of SSA or access SSA Information Systems resources. It is important to note that due to the unique relationship with the DDSs, supplemental regulations / guidance, and policies specific to these operating units are coordinated and distributed through SSA's Office of Disability Determinations (ODD), in the Office of Operations.

When providing SSANet, the policy applies to all locations owned or leased by SSA. The Deputy Commissioner for Systems (DCS) designs and maintains SSA's communication technology infrastructure. Modifications to the IT infrastructure require authorization, as unauthorized modifications to the Information Technology (IT) infrastructure can have detrimental effects on network performance and may introduce security vulnerabilities.

In addition, this policy applies to all SSA components engaged in, or considering the outsourcing of, IT services to Cloud Service Providers (CSPs). This includes acquisition of cloud-based products and services from external CSPs

3.1 Communications Technology Policy

3.1.1 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 "*SSA Firewall Rules*". The SSA Firewall Rules document is restricted to a limited audience on a "Need-to-Know" basis.

3.1.2 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:

- No local user accounts are to be configured on routers.
- All routers must be configured in accordance with the approved security configuration baseline, including approved access controls (i.e., (b) (7)(E) [redacted]) and user authentication.
- Passwords must be encrypted.
- Passwords must be changed from the manufacturer default setting prior to deployment within the SSA infrastructure.
- Utilize SSA password standards when selecting passwords Credential Rules and Requirements).
- Network devices must be configured to disallow:
    - Incoming network packets at the perimeter of the router with an invalid origin address.
    - Internet Protocol (IP) directed broadcasts, which can cause Denial of Service (DoS) attacks, and bring resources down.
    - Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) small services, which can be exploited to gain information about the targeted system.
    - Source routing, enabling IP spoofing.
    - Web services running on the router.
- Access rules for network control devices must be added as business needs arise.
- All network control devices must be listed within the corporate (b) (7)(E) [redacted] with a designated Point of Contact (POC).
- SSA network control devices must display an approved "agency attestation" (login banner) before granting access to the device. See ISP : Section 2.1 Information Systems Logical Access Control, ISP 2.1.1.5 Access Management, for detailed requirements.
- Routers must use SSA standardized Simple Network Management Protocol (SNMP) community strings. SNMP must be configured as followed:

- SNMP service must be disabled for devices not requiring use of SNMP.
- Non-blank, non-default SNMP community strings must be used.

NOTE

Some devices have default SNMP community strings hard-coded. This vulnerability should be mitigated (e.g., by blocking or filtering SNMP traffic at switch ports, upgrading firmware to a non-vulnerable version.

3.1.3 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. Form SSA-467, *Modem Registration Form* must be used for:

- Modem registration (including but not limited to telephone, Integrated Services Digital Network (ISDN), cable, and Digital Subscriber Line (DSL)).
- Modems in SSA facilities (including those by contractors, vendors, or the Office of Inspector General (OIG)).

3.1.4 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 subchapter 3.1.9 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 the Division of Security Customer Service (DSCS) 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.

3.1.5 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.

Unless using an authorized application, the use of other web conferencing or "webinar" technology (Webcast / Web conferencing / collaboration) on SSANet is prohibited due to the potential of unauthorized remote control of participating systems.

3.1.6 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.

3.1.7 Restricted Hardware

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.

3.1.8 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.

Remote access must conform to / comply with all Federal statutory requirements (see Office of Management and Budget (OMB) Memorandum M-06-16, which states that Federal agencies are to "Allow remote access with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access," and Homeland Security Presidential Directive 12 HSPD-12.)

SSA must:

- Limit remote access to approved agency solutions (e.g., VPN w/PIV cards).
- Employ automated mechanisms to monitor and control use of remote access methods.

3.1.9 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.

3.2 Wireless Technology

3.2.1 Approved Wireless Technology

The following are authorized in SSA's infrastructure:

- SSA-managed and issued smartphones (including BlackBerry Devices) and cellular telephones;
- Conventional cordless telephones;
- Commercial and residential wireless networks (e.g., public hotspots, hotels, home networks), and cellular Internet access can be used 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 (ISP 3.1.9 Multi-Homing).
    - Users are legally authorized to use the network, which is connecting to SSANet.
- 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. See ISP Section 3.4.5.

3.2.2 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.

3.2.3 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.

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

3.2.4 Prohibited Wireless Technology

The following wireless technology is prohibited:

- P2P communication technology (also known as ad hoc mode); wireless multifunction devices, network attached storage devices, wireless access points, routers, and other devices for connecting wireless stations must have ad hoc mode disabled.
- Linking devices to each other using wireless technology, with the exception of approved wireless applications and telecommunications links, or connecting an agency computer to an agency-issued smartphone / BlackBerry (ISP 3.1 ,Communications Technology Policy).
- Establishing an unauthorized wireless access point, this prohibition includes wireless access points that connect to agency procured broadband connections, commonly referred as off-network connections.

3.2.5 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.

3.3 Mobile Device Security

3.3.1 Background

For Mobile Device Security, the policy covers all SSA cell phones, and mobile computing devices.

All SSA cellular phones and mobile computing devices must be:

- On the authorized hardware list.
- On the authorized platforms list.
- On the authorized desktop / server software list.

- Permitted through a documented approved exception.

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.

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

3.3.2 International Travel

International travel is defined as travel conducted outside the continental United States, Alaska, and Hawaii. Individuals holding security clearances see (Additional Information).

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).

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.

3.4 Hardware, Software, and Platform Configuration

3.4.1 Background

Configuration management standards are the first line of defense for the prevention of malicious activities on SSA networks. Both Federal and private sector agencies recognize malicious software as a vector for potentially destructive attacks. Uncontrolled proliferation of unauthorized software and hardware negatively affects SSA's security posture. Unauthorized software can defeat security safeguards and settings, either inadvertently or maliciously. It is critical that all hardware, software, and platforms have configuration guidelines and standards so that they can be configured properly to ensure effective security.

3.4.2 Directive

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.

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

3.4.3 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 / server software list.

- Permitted through a documented approved exception.

At an employee's Alternate Duty Station (ADS), personal keyboards, monitors / TVs, and mice may be used as long as they do not require the interactive installation of unauthorized drivers or other software on an SSA-imaged machine. To determine whether a device requires the interactive installation of unauthorized drivers, see DTO's Unauthorized Drivers.

All installed software or hardware must follow security configuration standards.

3.4.4 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.

3.4.5 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.

3.5 Web Services Security

3.5.1 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. A Web Service has an interface described in a machine-processable format (specifically Web Services Definition Language (WSDL)). Other systems interact with the Web Service in a manner prescribed by its description using Simple Object Access Protocol (SOAP) messages, typically conveyed using Hypertext Transfer Protocol (HTTP), with an eXtensible Markup Language (XML) serialization in conjunction with other Web-related standards.

Authentication processes must ensure that the sender and recipient of the data are known to each other.

- Data access controls incorporates users authorized to send and receive information may do so. 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 6.3 Encryption Policy).
- For certificates presented to authenticate clients, SSA must trust the Certificate Authority for certificate revocation.

- If a certificate is fraudulently used, or a Certificate Authority's signing certificate is revoked, or at the request of the CIO or CISO, certificates must be disabled for use with SSA services.

- All audit requirements pertinent to the Agency must be adhered to (ISP 4.4.2 Audit Requirements and Guidelines).
- 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.

3.5.1.1 External Clients (Accessing SSA Web Services from Other than SSANet)

- Externally facing Web Services require a certificate-based server-to-server authentication process; the organizational credential would always be required for access to the Web Service. Exclusion to this policy allows for the elimination of the certificate-based server-to-server authentication if the Authentication Risk Assessment (ARA) determines that the Web Service requires Level 2 authentication, 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

- Credentials for External Clients:

  - Organizational Credentials (Multiple Clients Sharing a Single Credential):

    - Must be issued to an individual representing an organization and used for Web Services, thereby maintaining organizational accountability.
    - Can access more than one Web Service (application).
    - Roles assigned to credentialed individuals cannot be assigned to an organizational credential. For example, a credentialed organization that has access to Web Service A and Web Service C cannot have access to Web Application B, for which access to an individual credential has been issued.
    - For an individual with accountability for an organizational credential who wants to access SSA services for individuals, he / she must need to sign up for an individual credential.
    - Re-certification must occur in a period no greater than two (2) years.
    - Change of contact information invokes the recertification process at any time.
    - Are transferable.
    - Require an out-of-band notification (letter) to the organization informing them that an individual has registered for the Web Service role on behalf of the organization.

  - Individual Credentials (Single Client):

  - Must be issued to an individual representing themselves and used for Web Services.
  - Certificates must be registered and associated with the credential, and not on any credential provider revocation list.
  - Re-certification must occur in a period no greater than two (2) years.

- 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).

3.6 Cloud Security

3.6.1 Background

This subsection applies to all SSA components engaged in, or considering the outsourcing of, IT services to CSPs, as well as any acquisition of cloud-based products and services from external CSPs.

3.6.2 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 Management Act FISMA requirements, Federal Risk and Authorization Management Program (FedRAMP) requirements, and any additional agency requirements contained within this ISP.

3.6.2.1 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).

3.6.2.2 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 (see FedRAMP Security Controls).

- 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.

3.6.3 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.

3.6.4 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 Enterprise Support Architecture & Engineering (OESAE), 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.

3.7 References

GSA FedRAMP

3.7.1 SSA

- Security Authorization Process for External Systems

- Memo to CIOs, Security Authorization of Information Systems in Cloud Computing Environments

3.7.2 NIST

- NIST SP 800-145, The NIST Definition of Cloud Computing
- SP 800-46 Rev. 1, Guide to Enterprise Telework and Remote Access Security, June 2009
- SP 800-48, Guide to Securing Legacy IEEE 802.11 Wireless Networks, July 2008
- SP 800-121 Rev. 1, Guide to Bluetooth Security, June 2012

3.7.3 OMB

- Circular A-123, "Management Accountability and Control"
- Circular A-130, "Management of Federal Information Resources"
- Circular A-130, Appendix III, "Security of Federal Automated Information Systems"
- Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information

3.7.4 Laws and Regulations

Federal Managers' Financial Integrity Act of 1982, (Public Law 97-255), 31 U.S.C. §662 (1982)

4 Section IV: Information Security Risk Management

Introduction: OMB Circular A-130, and Federal Information Security Management Act of 2002 (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.

It is important to understand the nature and degree to which organizations, mission / business processes. Information Systems are vulnerable to identified threat sources, as well as whether or not the identified threat events, can be initiated by those threat sources.

Purpose: 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

Scope: All SSA employees, Disability Determination Services (DDS) employees, temporary staff, contractors, and other users when they act on behalf of SSA or access SSA Information Systems resources are required to participate in identifying potential risks, contribute to the implementation of appropriate mitigation strategies to address risks, and review and refer to the SSA Risk Management Framework. It is important to note that due to the unique relationship with the DDSs, supplemental regulations / guidance, and policies specific to these operating units are coordinated and distributed through SSA's Office of Disability Determinations (ODD), in the Office of Operations.

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).

4.1 Application and Device Event Logging

4.1.1 Scope

This policy applies to all applications and devices on the SSA Network.

4.1.2 General 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)

4.1.3 Events to be Logged

- 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 (referenced in the General Event Logging Requirements) must be applied.
- Application or device specific events to be logged must be identified in the system's Audit Plan.

4.1.4 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.

4.1.5 Review and update

Application and device owners must:

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

4.1.6 Access to Event Log

Access to event logs must be restricted using the least privilege and need to know concepts, as defined in Section 2.1.1.5 and Section 6.1.5.

4.1.7 Formatting 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 ^SOC for initial log setup, storage, and alerting guidance.

4.1.8 File Integrity Check Required

Category	Low Impact System	Moderate Impact System	High Impact System
No Sensitive Data	Optional	Yes	Yes
Sensitive Data	Yes	Yes	Yes

4.1.9 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.

4.1.10 Categorization

All systems must be categorized based on the type of data processed by the information system and the system categorization level (See ISP section 6.1.4 for categorization information).

4.1.11 Requirements

SSA Log Requirements – With no Sensitive Data (see ISP Section 4.1.12)

Category	Low Impact System	Moderate Impact System	High Impact System
Online Log Data	1 – 2 Weeks	1 -3 Months	3 – 12 Months
Log Data Rotation	Once a week or 25 MB in size	6 – 24 hours or 2 – 5 MB in size	15 – 60 minutes or 0.5 – 1.0 MB in size
Transfer to Central System	3 – 24 hours	15 – 60 minutes	At least every 5 minutes
Offline Log Data	At least 30 Days	At least 90 Days	1 Year
Analyzed by Owner	1 – 7 Days	24 hours	12 – 24 hours

SSA Log Requirements – With Sensitive Data (see ISP Section 4.1.12)

Category	Low Impact System	Moderate Impact System	High Impact System
Online Log Data	7 Days	7 Days	7 Days
Log Data Rotation	Once a week or 25 MB in size	6 – 24 hours or 2 – 5 MB in size	15 – 60 minutes or 0.5 – 1.0 MB in size
Transfer to Central System	3 – 24 hours	15 – 60 minutes	At least every 5 minutes

Offline Log Data	At least 30 Days	At least 90 Days	7 years
Analyzed by Owner	1 – 7 Days	24 hours	12 – 24 hours

4.1.12 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 6.1.7)

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 6.1.4)

4.2 Risk Management for IT Systems and Inventory

4.2.1 Inventory

FISMA and the Paperwork Reduction Act Section 3505 require Federal agencies to maintain a current inventory of their IT Systems. SSA has developed, and maintains a current inventory of IT Systems. The Office of Information Security (OIS) works with Security Authorization Managers (SAMs) and the Offices of Enterprise Support Architecture & Engineering (OESAE) 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.

Each of SSA's major reportable systems has an assigned SAM. It is the SAM's responsibility to determine if the Systems Security Plan (SSP) is current, as it is considered to be a "living document". In addition, the SAM is responsible for the security controls for the system and their adequacy for protecting the information during both the operation and decommissioning phase. The SAM must account for each subsystem that is both assigned to, and removed from, the major system. The SAM accurately updates this change to the subsystem inventory in the SSP.

4.2.1.1 New IT Systems and Inventory

All of the SSA major IT Systems have been rated and assigned an impact level per NIST Federal Information Processing Standard (FIPS) 199. Although SSA does not have a "High" impact-level system, the information in SSA systems is "sensitive" and requires adequate security controls per NIST SP 800-53, rev. 4.

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 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 PRIDE (ISP 4.2.3.1 Project Resource Guide (PRIDE)). This includes ensuring the security tasks (SSPs, Security Controls Testing, and Risk Assessments) in the life cycle process are carried out. PRIDE explains the importance of the new system being recorded in the Application Portfolio Manager (APM).

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.

4.2.1.2 Existing IT Systems Inventory

For existing systems, the risk assessment process must be performed at least every three (3) years for all enterprise level Federal Information Systems. A risk assessment must also be performed on these applications if a major change occurs. A major change is defined as:

- Installation of a new or upgraded operating system, middleware component, or software application.
- Modifications to systems ports, protocols or services.
- Installation of a new or upgraded hardware platform or firmware component.
- Modifications to cryptographic modules or services.

Complete risk assessments must be conducted prior to requesting Security Authorization for a system if one has not been done in the last three (3) years. Security controls must be integrated throughout the SDLC (see PRIDE for more detailed information).

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.

4.2.2 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".

4.3 Integrating Security into the SDLC

4.3.1 Background

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".

To be most effective, Information Security must be integrated into the SDLC from system inception. There are three (3) important aspects of security in relation to the SDLC:

- Security must be considered from the first to the last phase of the system's life cycle.
- Development of security is a repetitive process. As the system progresses through each phase of the life cycle, identified vulnerabilities are mitigated through the selection and implementation of safeguards.
- All security considerations should be documented in the standard SDLC documents.

4.3.2 Procedure

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:

1. Categorize the System and Select Security controls.
2. Document, Implement, and Assess Security Controls.
3. Authorize the Information System.
4. Monitor Security Controls.
5. Ensure orderly termination of the system.

4.3.3 Systems

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 PRIDE. PRIDE 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.

4.3.3.1 Project Resource Guide (PRIDE)

The official SDLC roadmap that SSA follows when it develops software tools or applications is available on PRIDE. This includes requirements development, appropriate timeframes, and sample template documents. SDLC related security considerations on PRIDE 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.

4.3.3.2 Waivers

Temporary waivers to SSA policy may be considered on an individual basis with justification identifying the business need and impact (ISP Appendix A Request for Waivers from ISP Policy).

4.3.4 Security and the System Development Life Cycle (SDLC)

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.

4.3.4.1 Identifying Systems Changes that may Require Security Changes

The PM is responsible for notifying his / her CSO when they are assigned a systems development project, and meeting with the CSO to discuss possible security issues. As the CSO becomes aware of these requests, he / she notifies the Chief Information Security Officer (CISO), the Office of Operations (DCO), any other CSOs whose components must be involved in implementing the project, and any other components with an interest in the system's security. For example, the Office of Disability Determinations (ODD) would have an interest in the security functionality built into disability systems. OIS has developed a "Significant Change Reporting Guidance and Questionnaire" that is forwarded to each SAM for their review and updated on a yearly basis.

4.3.4.2 Analyzing the Security Implications

Analysts from each involved security staff examine the information available about the proposed systems functionality to determine the control requirements. All major SSA components participate in examining the functionality to determine which positions within their components require what access for a particular application.

The CISO provides the security policy perspective, as well as interpreting audit and integrity review requirements in consultation with other involved components. The CISO also examines the functionality to determine whether additional internal controls, such as a two (2) Personal Identification Number (PIN) process, are required.

4.3.4.3 Security Personnel Meeting

Subsequent to each component having an opportunity to examine information on the system, the various security personnel (CSO, PM) discuss the specific controls needed for the system. These discussions can be formal meetings, such as the Security Kickoff meetings for access control, and the Audit Planning and Audit Steering Group meetings, or informal discussions by phone. These discussions ensure that the controls recommended for the system meet the needs of all of the involved components.

4.3.4.4 User Needs Statements

Based on the Security Team discussions, user needs statements are prepared. These statements form the basis for the requirements documents prepared by DCS. Included in the user needs statements are access controls, audit and integrity review statements, and other controls.

4.3.4.5 Functional Requirements and Validation Plan

The Functional Requirements documents and the Validation Plans for security functionality are written by the application's System Project Management Team or DCS Security Staff. Access control matrices are reviewed by DCS and then the necessary Top Secret profile modifications are made.

4.3.4.6 Development and Authorization of Security Features

Security functionality is developed in conjunction with all other system functionality. If changes are made to the application affecting the types of security controls that are needed, then the security controls are also changed.

After development is complete, the security functions, along with all other system functionality are validated in accordance with the Validation Plan that was prepared by DCS during the requirements definition process. A Validation Checklist is completed to document completion of each validation task. If any requirement is not met, the software must go back to the programming staff for corrective action. At the end of the system validation process, the validated system is approved for release to production. The system must meet Agency policy requirements to be approved and released to production. The Systems Release Certification

document contains the certification documentation supporting the software's release to production.

4.3.4.7 Systems Implementation and Operation

As each new system is implemented, security officers in the operational components watch for potential security problems with application, report those problems to the CSO, and the DCS lead security analyst for resolution.

A compilation of lifecycle products for the system is maintained and available for review by auditors, providing complete information on the application's development, including the security functions.

Each application system is subject to a reauthorization process, during which the application, including its security functions, is examined to ensure that it still meets SSA's security objectives. The reauthorization process occurs the sooner of: once every three years or when a significant change takes place (see NIST SP 800-37 revision 1, Appendix F, Security Authorization, Subsection F.6, Event-Driven Triggers, for an explanation of what may constitute a significant change.

4.3.5 Web Application Development Policy

4.3.5.1 Background

This segment 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 policy complies with both Federal regulations and business requirements.

4.3.5.2 Web Application Development Rules

The 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. Internet usage is governed by SSA's Personal Use of Government Equipment policy.

The following requirements apply to the project managers and developers for **Internet** applications:

- Use the agency approved static code analysis tool to evaluate source code This includes, but is not limited to new releases, major releases, maintenance releases and emergency releases.
- OIS determines if applications require a penetration test in the validation environment.
- (b) (7)(E)
  - [redacted]

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

- Persistent cookies are not allowed.

The following requirements apply to intranet project managers and developers of **Intranet** applications:

- Are accessed by internal users (inside SSA's firewalls) and it is recommended for these applications to use the agency's static code analysis tool to scan source code for security vulnerabilities.
- Cookies are allowed (subject to the restrictions stated below).
  - Can only contain functional information that is necessary to improve, enhance, or customize the user experience.
  - Cannot contain any type of Personally Identifiable Information (PII) including, but not limited to, Names, Social Security Numbers, Account Numbers, Credit Card Numbers, and Telephone Numbers.
  - Cannot contain any type of credential or logon information or allow for any type of automatic logon.
  - Should have the shortest expiration date practical, but in all cases the maximum expiration date cannot be greater than one (1) year.

The following requirements are common to both **Internet and Intranet** applications:

- Developers must follow best coding practices 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 form fields input
  - Use proper access controls
  - Manage authentication
  - Identify and handle error conditions

For additional development guidance, please see the Division of Technical Operations (DTO) Software Development Security webpage.

4.4 Selected Security Controls

A. Application Controls (1-7)

1. Transactions are authorized – Management must authorize information entered into Automated Information Systems (AISs).
2. Transactions are valid – AISs must process only data that represent legitimate events.

3. Information is complete – Only valid data may be processed by an automated Information System.
4. Information is accurate – Data must be free from error during all phases of processing, within defined levels of tolerance.
5. Information is timely – Data must reflect the correct cycle, version, or period for the processing being performed. Financial management data must be recorded as soon as practical after the occurrence of the event, and relevant preliminary data must be made available to managers promptly after the end of the reporting period.
6. System and data are secure – Data files, computer programs, and equipment must be kept secure from unauthorized changes, accidental changes, unauthorized disclosure and use, and physical destruction. Detective and corrective controls may also apply, depending on the sensitivity level designation of system data.
7. System is auditable – An information trail must exist that establishes individual accountability for transactions and permits an analysis of breakdowns and other anomalies in the system.

B. General Controls (8-33)

8. System controls exist – The control system for each automated Information System must ensure that appropriate safeguards are incorporated into the system, tested before implementation, and tested periodically after implementation.
9. Five-year system plan is developed – Each Agency must develop a plan, including specific milestones with obligation and outlay estimates, for every automated Information System in the Agency. This requirement covers both existing automated Information Systems and systems under development.
10. Contingency plan / disaster recovery plan exists – Agencies must develop, maintain, and test disaster recovery and continuity of operations plans for their data center(s) to provide reasonable continuity of data processing support if normal operations are prevented.
11. Vulnerability assessment is conducted – Agencies must review the susceptibility of their programs or functions to waste, loss, unauthorized use, or misappropriation, by conducting vulnerability assessments or equivalent studies, such as audits.
12. Cost-benefit analysis exists – Agencies must determine and compare the benefits of proposed systems or controls against the cost of developing and operating those systems or controls. Only proposals for which the expected benefits exceed the estimated costs by 10 percent should be considered for development, unless otherwise equates to a satisfactory level of confidence, based on management's judgment of the cost / benefits of controls versus recognized risks. It is recognized that it is not cost-effective to attain 100 percent assurance. Each Agency must provide reasonable assurance.
13. Reasonable assurance is applied – Reasonable assurance equates to a satisfactory level of confidence, based on management's judgment of the cost / benefits of controls versus recognized risks. It is recognized that it is not cost-effective to attain 100 percent assurances. Each Agency must provide reasonable levels of assurance.

14. Control objectives are defined – Agencies must establish goals to address known vulnerabilities, or to promote reliability or security of automated Information Systems.
15. Control techniques are selected – Agencies must develop methods to satisfy control requirements by preventing, detecting, and / or correcting undesired events.
16. Adequacy of security requirements is determined – Agencies must ensure that appropriate technical, administrative, physical, and personnel security requirements are included in specifications for the acquisition or operation of automated Information System facilities, equipment, or software.
17. Security specifications exist – Internal control and security requirements must be stated as design specifications and approved by management before application systems development begins.
18. Adequacy of security specifications is determined – Agencies must present proof to management that design specifications satisfy control requirements to authorize computer program development and / or modifications (programming).
19. System design is approved – Before development (programming) of an automated Information System is authorized, management must be assured that the system design satisfies user requirements and incorporates the appropriate control requirements. The design review must be documented and be available for examination.
20. Controls are documented – Internal control systems, including all transactions and significant events, must be clearly documented and readily available for examination.
21. System documentation exists – Documentation must reflect the current state of an automated Information System as it is being operated. The documentation must be sufficient to ensure effective operation by users and system maintenance by programmers.
22. System contingency plan exists – Plans must be developed, documented, and tested to assure that the users of automated Information Systems can continue to perform essential functions in the event that processing capability is interrupted. The plan must also be consistent with the Agency-wide disaster recovery plan.
23. Controls are tested – Before a new or modified automated Information System is placed into production status, its controls must be tested to prove that they operate as intended. The test results must be documented and sent to management for approval prior to implementation of the system.
24. System test is conducted – Before implementation of an automated Information System is authorized, evidence that the system operates as intended must be presented to management. This evidence must also include the results of controls testing. The test results must be documented and available for examination.
25. Test results are documented – Documentation must demonstrate that the control and functionality requirements of automated Information Systems operate as intended.
26. System is certified prior to implementation – Before an automated Information System can be implemented, an Agency official must certify that the system meets all applicable Federal policies, regulations, and standards, and that test results demonstrate that installed controls are adequate for the system.

27. Controls review is performed – Periodically, each automated Information System must be tested to determine if its controls still function as intended. The results of these tests must be documented and available for examination.
28. Periodic reviews and recertifications are conducted – At least once every three (3) years, Agencies must review their automated Information Systems and recertify the adequacy of their safeguards. The recertifications must be documented and available for review.
29. Periodic risk assessments are conducted – Agencies must conduct periodic risk assessments at their automated information facilities to provide a measure of the relative vulnerabilities and threats to the facilities so that security resources can be effectively distributed to minimize potential loss.
30. Corrective action is taken; audit findings are resolved promptly – Managers must promptly evaluate audit findings and recommendations, determine proper corrective actions, and complete those actions.
31. Annual report on internal controls is prepared – Each Agency must annually determine if its systems of internal controls are in compliance with the Comptroller General's standards.
32. Annual report on accounting systems is prepared – Each Agency must annually determine if its accounting systems are in compliance with the Comptroller General's standards.
33. Annual reports are sent to the President – The head of each Agency must sign annual reports and transmit them to both the President and Congress.

C. Administrative Controls (34-45)

34. Organizational responsibility is affixed – The Agency must assign responsibility for planning and directing the controls evaluation process for the organization. The programs and functions conducted in each organizational component must also be specified.
35. Separation of duties exists – Key duties and responsibilities in authorizing, among processing, recording, and reviewing transactions must be separated among individuals.
36. Supervision is provided – Qualified and continuous supervision must be provided to ensure that control requirements are met.
37. Supportive attitudes exist – Managers and employees should maintain and demonstrate a positive and supportive attitude toward controls at all times.
38. Personnel are competent – Managers and employees should demonstrate personal and professional integrity and maintain a level of competence that allows them to accomplish their assigned duties, and to understand the importance of developing and implementing good controls.
39. Security training program exists – Agencies must establish a security awareness and program so that Agency and contractor personnel involved with automated Information Systems are aware of their security responsibilities and know how to fulfill them.

40. Written policies and procedures exist – Each agency must establish administrative procedures to enforce the intended functioning of controls, and to ensure that performance appraisals reflect execution of control-related responsibilities.
41. Personnel security policies exist – Each agency must establish and manage personnel security procedures, including requirements for screening agency and contractor personnel involved in the design, development, operation, maintenance, or use of automated Information Systems. The level of screening depends on the sensitivity level designation of system data. Additionally, the February, 1996 revision of OMB Circular A-130, requires that agencies establish a comprehensive set of Rules of Behavior for all personnel setting forth the behavior expected to ensure compliance with stated security policy.
42. Individual responsibilities are affixed – Assignments of responsibility must be made for internal controls, accounting systems, and data center security on an agency-wide and individual system/center basis.
43. Custody and accountability are assigned – Each official whose function is supported by an automated Information System is responsible and accountable for the products of the system.
44. Record retention procedures exist – Each agency must establish procedures for the retention, archiving, and destruction of data files.
45. Release of information is provided for – Each agency must have procedures in place so that information can be extracted from systems to meet requests made under the Privacy Act and the Freedom of Information Act (FOIA).

D. Required System Functions (46-55)

46. System is efficient – The benefits of an AIS must exceed the costs to develop or operate the system.
47. System operation is economical – Uneconomical systems must be identified and phased out.
48. System is effective – Periodically, each automated Information System must be reviewed to determine if the system still meets organizational needs.
49. System supports management – Data must be recorded and reported in a manner that facilitates the fulfillment of responsibilities of both program and administrative managers.
50. System supports budget – Financial management data must be recorded, stored, and reported to facilitate budget preparation, analysis, and execution.
51. Comparability/consistency is provided for – Financial management data must be recorded and reported m the same manner throughout an Agency, using uniform definitions that are synchronized with budgeting for each reporting period.
52. System is useful / relevant – Data capture and reports must be tailored to specific user needs, and, if usage does not justify costs, the data or reports must be terminated.
53. System provides full disclosure – Data must be recorded and reported in a manner that provides users of the data with complete information about the subject of the report, in

accordance with Office of Management & Budget (OMB), Treasury, and Privacy Act standards.

54. Individual access is allowed – Information about an individual contained in a database must be extracted in response to a request by that individual or his / her representative, when required by the Privacy Act.
55. Network compatibility exits – All new AISs developed or acquired must be compatible with any existing systems that must be linked to the new system.

Exhibit A provides the control requirements referenced to major control directives in matrix format.

Exhibit A – Control Requirements Cross Referenced to Major Control Directives

Item No.	Requirements	OMB A-123	OMB ICG	OMB A-127	OMB A-130	GAO Title II	FMFIA	Privacy Act
A	**APPLICATION CONTROLS (1-7)**							
1	Transactions are authorized.	X	X		X	X		X
2	Transactions are valid.	X	X		X	X		
3	Information is complete.	X	X	X		X	X	X
4	Information is accurate.	X	X	X	X	X	X	X
5	Information is timely.	X	X	X		X	X	X
6	System and data are secure.				X		X	X
7	System is auditable.			X		X		
B	**GENERAL CONTROLS (8-33)**							
8	System controls exist.				X	X		
9	Five-year system plan is developed.			X	X	X		
10	Contingency plan/disaster recovery plan exists.				X	X		
11	Vulnerability assessment is conducted	X	X			X		
12	Cost/benefit analysis exists.					X		X
13	Reasonable assurance is applied.	X	X	X	X	X	X	
14	Control objectives are defined.	X	X			X		
15	Control techniques are selected.	X	X			X		
16	Adequacy of security requirements is determined.				X			X
17	Security specifications exist.				X	X		
18	Adequacy of security specifications is determined.				X			
19	System design is approved.					X		
20	Controls are documented.	X	X			X		
21	System documentation exists.					X		
22	System contingency plan exists.				X	X		

Exhibit A – Control Requirements Cross Referenced to Major Control Directives

Item No.	Requirements	OMB A-123	OMB ICG	OMB A-127	OMB A-130	GAO Title II	FMFIA	Privacy Act
23	Controls are tested.				X	X		
24	System test is conducted.					X		
25	Test results are documented.				X	X		
26	System is certified prior to implementation.				X			
27	Control review is performed.	X	X	X		X	X	
28	Periodic reviews and recertifications are conducted.			X	X	X		X
29	Periodic risk assessments are conducted.					X		
30	Corrective action is taken; audit findings are resolved promptly.	X	X			X		
31	Annual report on internal controls is prepared.		X	X		X		
32	Annual report on accounting systems is prepared.					X	X	
33	Annual reports are sent to President.	X	X		X	X	X	
C	**ADMINISTRATIVE CONTROLS (34-45)**							
34	Organizational responsibility is affixed.		X					X
35	Separation of duties exists.	X	X			X		
36	Supervision is provided.	X	X			X		
37	Supportive attitudes exist.	X	X			X		
38	Personnel are competent.	X	X			X		
39	Security training program exists.				X			
40	Written policies and procedures exist.	X	X	X				X
41	Personnel security policies exist.				X			
42	Individual responsibilities are affixed.	X	X	X	X	X		
43	Custody and accountability are assigned.	X	X		X	X	X	
44	Record retention procedures exist.							X

Exhibit A – Control Requirements Cross Referenced to Major Control Directives								
Item No.	**Requirements**	**OMB A-123**	**OMB ICG**	**OMB A-127**	**OMB A-130**	**GAO Title II**	**FMFIA**	**Privacy Act**
45	Release of information is provided for.							X
D	**REQUIRED SYSTEM FUNCTION (46-55)**							
46	System is efficient.			X		X		
47	System operation is economical.			X		X		
48	System is effective.				X	X		
49	System supports management.			X				
50	System supports the budget.			X		X		
51	Comparability/consistency is provided for.			X		X		
52	System is useful / relevant.			X	X	X		X
53	System provides full disclosure.			X		X		X
54	Individual access is allowed.				X		X	X
55	Network compatibility exists.				X			

4.5 Implementation of Security Controls

4.5.1 Background

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.

4.5.2 Audit Requirements and Guidelines

The Audit Plan should be completed in conjunction with required FISMA documentation during the applicable stage outlined in the PRIDE process. For more information regarding the SDLC and PRIDE process see http://pride.ssahost.ba.ssa.gov/Construction/internal_control.cfm.

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.

4.5.2.1 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:

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

NOTE

Sensitive information provided by internet users such as their passwords and answers to personal security questions should not be maintained in the audit record.

4.5.2.1.1 Access to Audit Data

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.

4.5.2.1.2 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.

4.5.2.1.3 Distribution of Audit Data

Distribution of audit trail data is restricted to security staff in OIS, OQP, 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 their security and integrity review responsibilities, and with the OIG in support of its 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 1.7.2, Role-based Training for Individuals with Significant Information Security Responsibilities) for more information.

4.5.2.1.4 Retention Periods for Audit Data

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).

4.5.2.1.5 (b) (7)(E)

(b) (6), (b) (7 is one of SSA's official repositories for audit trail data. Authorized users may access resources pertaining to the (b) (7)(E) at OIS's secure site at (b) (7)(E) This site includes the (b) (7)(E) 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.

4.5.2.1.6 (b) (7)(E)

(b) (7)(E) 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 (b) (7)(E) should be used. Web developers may choose to use the (b) (7)(E) to meet auditing requirements. Further information about (b) (6), (b) (7)(E) can be found at (b) (6), (b) (7)(E)

4.5.2.1.7 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.

4.5.2.1.8 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.

4.5.2.1.9 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.

4.5.2.1.10 Individuals of Extraordinary National Prominence (IENP) Requirements

SSA employees, contractors and data sharing partners using SSA systems are prohibited from accessing records belonging to IENP. All SSA applications must implement the IENP Block; the following information needs to be captured when the IENP Block is implemented. Additional information about implementation can be found at the Develop Security Design & Internal Controls Requirements site http://pride.ssahost.ba.ssa.gov/Construction/internal_control.cfm.

- 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. Developers should work with their CSO to develop a process that prevents such incidents. For special circumstances that would involve not implementing the IENP block, please refer to ISP Appendix A, Requests for Waivers from Information Security Policy (ISP) Policies, for information regarding the waiver process. Additional information regarding IENP can be found in the Program Operating Manual System (POMS).

4.5.2.1.11 Own SSN Requirements

SSA employees, contractors and data sharing partners using SSA systems are prohibited from accessing their own SSN or any record where their SSN is present. All SSA applications that access client data must implement the Own SSN Block, developers should work with their CSO to develop a process that prevents such incidents. The following information needs to be captured when the OwnSSN Block is implemented. Additional information about

implementation can be found at the Develop Security Design & Internal Controls Requirements site http://pride.ssahost.ba.ssa.gov/Construction/internal_control.cfm

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

4.5.2.1.12 Integrity Review Process

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).

4.5.2.1.13 SDLC & PRIDE

The project team must follow the SDLC guidelines in the PRIDE process when implementing audit trail requirements and/or policy. The project team must complete the necessary FISMA documentation as well as completing a system specific Audit Plan during the applicable stage outlined in the PRIDE process. ISP 4.2, Integrating Security into the SDLC, provides an overview of SDLC policy. For additional information regarding the PRIDE process, refer to http://pride.ssahost.ba.ssa.gov.

4.5.2.1.14 Separation of Duties

After evaluating their business process for risks, systems owners can choose from a number of possible solutions to implement separation of duties controls. A system must have access controls to restrict who can access the system, using the concept of "Least Privilege" and "Need to Know".

4.6 Systems Security Assessment and Authorization (SSA&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.

4.6.1 Personnel

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.

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.

4.6.1.1 Security Authorization Package (SAP)

The Security Authorization Package (SAP) is used to assist the authorizing official with making credible, risk-based authorization decision for the operation of any SSA Information System. Authorization must be attained prior to full implementation and whenever significant changes are made to the system. The SAP is required to demonstrate that appropriate security controls exist to safeguard the system and must contain the following documents:

Security Assessment Report (SAR)

The SAR must be used to document the results of the security controls assessment and provide recommended corrective actions for any vulnerabilities or deficiencies in the Information System identified during the assessment.

Risk Assessment Report (RAR)

The RAR provides information on threats, vulnerabilities, and potential impacts to the system, as well as the analyses for the risk mitigation recommendations. The risk assessment must be performed at least every three (3) years or sooner if significant change to the Information System or its operating environment occurs. The risk assessment should follow the guidelines in NIST SP 800-30, Rev. 1 – Guide for Conducting Risk Assessments.

System Security Plan (SSP)

The SSP provides an overview of the information system security requirements and describes the security controls in place or planned, to meet those requirements. The SSP also contains a list of subsystems, supporting appendices, other risk and security related documents, and system interconnection agreements. The security safeguards implemented for the information system must meet the policy and security control requirements identified in the SSP.

The SSP should, 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 should 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.

Plan of Action and Milestones (POA&M)

The POA&M describes the specific tasks that are planned to correct any weaknesses identified during the security control assessment. The POA&M must define the specific tasks to be accomplished, milestones in meeting the tasks, required resources, and scheduled completion dates. The Information System SO must prepare the POA&M for the authorizing official based on the findings and recommendations in the SAR. The authorizing official uses the POA&M to monitor progress in correcting weaknesses identified during the security control assessment.

POA&M entries are not required when weaknesses are remediated during the assessment or prior to the submission of the authorization package to the authorizing official (ISP 4.5.2.1, Security Authorization Package (SAP) POA&M Information).

Authority To Operate (ATO) Recommendation – Letter 1

The ATO Recommendation Letter must be prepared by the SO's staff, addressed to the SSA CIO, and included in the SAP. The completed ATO Recommendation Letter must be signed by the SAM for the system, the designated SO, and the SSA agency-level officials who have agreed to share accountability for the system.

ATO CISO Recommendation – Letter 2

The CISO Recommendation Letter must be addressed to the SSA CIO and prepared by the CISO, who certifies that the contents of the SAP meet the requirements of the appropriate Federal regulations, standards, and guidelines and recommends a security authorization decision.

ATO Decision – Letter 3

The Decision Letter is prepared according to NIST SP 800-37, Rev. 1 – Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. The ATO Decision Letter must be signed by the SSA CIO, addressed to the appropriate SO, SAM, and sharing partners. The letter documents whether the system is authorized to operate or denied the authority to operate.

4.6.1.2 Shared Accountability

Multiple components may have shared sign off authority on each SAP for a major IT System. View the table for a breakdown of system ownership and sharing partner responsibilities: SSA Major Applications and General Support Systems.

4.6.2 Automated Information Systems (AIS) Contract Policy

4.6.2.1 Background

ISP 4.5.3 POA&M Process provides SSA system security policy requirements for developing AIS contracts and grants. AISs include any system that collects, processes, transmits, stores, or disseminates agency information. For detailed and specific procurement and contracting information status and regulations, see the Office of Acquisitions and Grants website. The following mandates require all Federal agencies to protect citizens' private information.

- Privacy Act of 1974
- Tax Information Security Guidelines for Federal, State, and Local Agencies
- Section 1106 of the Social Security Act
- Federal Acquisition Regulation (FAR) 52.239-1
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources

This subsection is directed to all SSA employees, employees of other agencies, contractors, temporary employees, business partners, and any other users with access to the SSA AISs.

4.6.2.2 Directive

Every solicitation, acquisition, or grant involving AISs or the use of SSA AIS resources must include appropriate security requirements.

All personnel involved with the contracting and grant process must integrate necessary security requirements into all phases of the acquisition cycle. These include the planning, solicitation, review of offer's proposals / quotes, the contract award, and contract administration. As used in this chapter, the term "contract" includes contracts, contract modifications, purchase orders, delivery orders, task orders, and grants. As used in this subsection, the term "contractor" includes contractors, subcontractors, and grantees.

4.6.2.3 Information Security Clauses for AISs

The following Information Security clauses are for inclusion in Statements of Work (SOWs) and awarded contracts where SSA information resources are being transmitted, processed, or retained.

- Security for this contractor-operated system must comply with security requirements prescribed by the National Institute of Science and Technology (NIST) under authority of the Federal Information Security Management Act (FISMA). The vendor must follow the methodology defined in NIST SP 800-37, Rev. 1 (Feb 2010), *Guide for Applying the Risk Management Framework to Federal Information Systems*, for implementing required security controls.
- The sensitivity level of the information to be processed, stored, and/or transmitted by the system must carry a security categorization as defined by (FIPS 199, (Feb 2004),

Standards for Security Categorization of Federal Information and Information Systems. The vendor must document the status of security controls described in NIST SP 800-53 Rev. 4 (April 2013), *Security and Privacy Controls for Federal Information Systems and Organizations,* for protecting the applicable impact level information as categorized by FIPS 199.

- The SO must subject the Information System to SSA's Security Assessment and Authorization Process, which must entail security testing and evaluation of the implemented security controls. The vendor must actively facilitate an on-site security assessment to determine the status of implemented security controls. Control failures could result in non-authorization until the vendor provides acceptable documentation that security control failures have been adequately remediated.
- The vendor must test the status of implemented security controls and provide the assessment results to SSA for inspection. SSA's security authorization of the vendor's system is dependent upon evidence that FISMA security control requirements have been satisfied. The vendor may need to conduct an independent security assessment every three years or prior to deploying major changes to the system infrastructure of functionality, dependent upon the security categorization as defined by FIPS-199.
- The contractor must prepare a System Security Plan (SSP) to document the implementation status of required security controls. The SSP must:

    - Incorporate all entities and agents of the contractor who must have access to sensitive information, including subcontractors.
    - Provide an overview of architecture and security requirements of the system used for collection, storage, maintenance, transmission, and disposal of sensitive information.
    - Describe the implementation status of all security controls required to protect moderate impact level information, including supporting rationale for the implementation status.

Additionally, the contractor must continuously monitor the status of implemented security controls to ensure their continued effectiveness. The contractor must demonstrate continuous monitoring by determining the security impact of proposed or actual changes to the Information System and its environment of operation; and recording relevant information about specific changes to hardware, software, firmware, environment (e.g., hosting networks, mission / business use of the system, threats), or risk management in the SSP. For changes affecting the security state of the system, the contractor must take corrective actions and revise appropriate documents, including the Security Assessment Report, SSP, and POA&M).

To ensure proper handling of sensitive information, the contractor must submit an SSP to SSA for the contractor's Information System for written approval before SSA transmits sensitive information to the contractor. The contractor must also enforce the following sensitive information handling requirements:

- Sensitive information is accessible only to persons satisfying personnel suitability determination requirements as prescribed in the suitability section of the contract.

- Restrict access to all sensitive information to the minimum number of individuals who need to perform the contract.
- Process all sensitive information under the supervision of authorized personnel that protects the confidentiality of records.
- Inform all personnel with access to sensitive information of the nature of the information and required safeguards to protect it.
- Any subcontracts that involve handling SSA sensitive information must include the same sensitive information handling requirements.
- For systems that handle Federal Tax Information (FTI), the contractor must consider adherence to IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies.

4.6.2.4 External Service Providers (ESPs)

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 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.

4.6.3 POA&M Process

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 ^OIS Assurance. 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.

(b) (7)(E) is the agency-wide authoritative source for tracking Information Security weaknesses, including critical infrastructure vulnerability assessments and security control assessments. (b) (7)(E) is maintained and administered by the Office of Information Security (OIS), and additional information about (b) (7)(E) is contained in the (b) (7)(E). The (b) (7)(E) 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 (b) (7)(E). Appropriate OIG personnel will be provided read-only access to POA&M information in (b) (7)(E). Information on POA&M update in (b) (7)(E) 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.

4.7 References

4.7.1 Department of Homeland Security (DHS)

Homeland Security Presidential Directive 12: Policy for a Common Identification Standard Federal Employees and Contractors

4.7.2 NIST

- SP 800-18, Rev. 1, Guide for Developing Security Plans for Information Technology Systems, Feb 2006
- SP 800-30, Guide for Conducting Risk Assessments
- SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- SP 800-53, Rev 4: Recommended Security Controls for Federal Information Systems and Organizations
- SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- FIPS 199 Standards for Security Categorization of Federal Information and Information Systems
- NIST SP 800-60 for Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-39 - Managing Information Security Risk Organization, Mission, and Information System View
- NIST SP 800-53 Rev 4 - Recommended Security Controls for Federal Information Systems and Organizations
- NIST SP 800-64 Revision 2 - Security Considerations in the System Development Lifecycle
- NIST SP 800-64 Security Considerations in the System Development Life Cycle
- Office of Acquisition and Grants (OAG)

- Office of Acquisition and Grants (Project Officer's Web Page)

4.7.3 Laws and Regulations

- Freedom of Information Act, Public Law (P.L.) 93-502, Amendments 1974
- Federal Information Security Management Act of 2002 (FISMA)

4.7.3.1 SSA

- SSA's Policy for Internet Project Development
- Form SSA- 468 Active X Waiver Request
- Personnel Policy Manual (PPM) S297 Implementation of the Privacy Act.
- Administrative Instructions Manual System (AIMS) General Administration, 09 External Affairs, Instruction 30 "SSA Internet Policies"
- SSA Internet / Intranet Standards and Guidelines
- SSA "Mainframe Administration Standards"
- SSA Project Resource Guide PRIDE Website
- ISP 4.2, Integrating Computer Security into the SDLC
- ISP 6.3, Encryption Policy
- ISP Appendix B: Roles And Responsibilities
- ISP 2.2, Systems Access Security Administration Software.
- ISP Appendix A: Requests for Waivers from Information Security Policy (ISP) Policies
- http://www.archives.gov/records-mgmt/grs/grs20.html - electronic records
- http://www.archives.gov/records-mgmt/grs/grs07.html - financial records
- http://www.archives.gov/records-mgmt/grs/grs24.html - references PKI records and 7 years

5 Section V: Contingency Planning and Incident Response

Introduction: 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 and incident response to be successful agency management must ensure the following:

- Understand the IT contingency planning policies and incident response plans have emphasis on maintenance, training, and exercising the contingency incident response plan.
- Understand the Incident Response (IR) and Contingency Planning (CP) Processes and it's 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.

Purpose: This section identifies the agency's planning principles and practices for developing and maintaining effective IR and CP. 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.

In addition, this section provides SSA Information Security policy governing the identification and processing of security incidents. This policy complies with Federal requirements, such as the Federal Information Systems Management Act of 2002 (FISMA) and Office of Management and Budget (OMB) circulars and directives.

Scope: This applies to all SSA employees, Disability Determination Services (DDS) employees, temporary staff, contractors, and other users who act on behalf of SSA or access SSA Information Systems resources. It is important to note that due to the unique relationship with the DDSs, supplemental regulations / guidance, and policies specific to these operating units are coordinated and distributed through SSA's Office of Disability Determinations (ODD), in the Office of Operations.

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

5.1 Contingency Planning Policy

5.1.1 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. SSA Information System Owner (SO) and Security Authorization Manager (SAM) must develop and maintain an ISCP.

The ISCP must address all Information System subsystems and clearly document the delineation point between the contingency planning responsibilities of the Information SO / SAM and those of any common control provider from which the system is inheriting contingency planning controls.

The ISCP must adhere with National Institute of Standards and Technology (NIST) Special Publication (SP) *Contingency Planning Guide for Federal Information Systems* 800-34, Rev.1, and address NIST SP Assessing Security and Privacy Controls in Federal Information Systems and Organizations (NIST SP 800-53A, Rev. 4).

The ISCP system must:

- Review and update the current:
    - Contingency planning policy [Assignment: organization-defined frequency], and
    - Contingency planning procedures [Assignment: organization-defined frequency].
- Identify essential mission's business functions and associated contingency requirements.
- Provide recovery objectives, restoration priorities, and metrics.
- Address contingency roles, responsibilities, and assigned individuals with contact information.
- Address maintaining essential missions and business functions despite an Information System disruption, compromise, or failure.
- Address eventual, full Information System restoration without deterioration of the security measures originally planned and implemented.

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.

5.1.2 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 for every General Support System (GSS) and MA (major applications) system. The plans must detail the process to restore the agency's critical operations to an acceptable level of functionality after a disruption of operations;
- 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 larger COOP process.

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 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

Anticipating Potential Contingencies or Disasters

Complete vulnerability assessments prior to COOP to identify all threats, which can affect resources. Consider all foreseeable threats, and the related impact on critical resources, in the planning process (see Risk Management Policy for more detailed information on this process).

Selecting Contingency Planning Strategies

When considering the need for a system Contingency Plan, evaluate the security controls implemented for the selected system. Strategies must also anticipate and include other possibilities such as the data stored for the application data becoming unavailable (an offsite backup data store should be available), or employees responsible for the system being unavailable (other employees should be trained to fill in), etc. Test recovery actions and backups on a periodic basis.

Implementing the Contingency Strategies

Implement and document contingency strategies for various contingencies and distribute to employees on a "Need-to-Know" basis.

Testing and Revising

Test the Contingency Plan annually and revise when required. The following is an example of a revised plan. A component's Contingency Plan requires transferring a critical workload from one Personal Computer (PC) to another. In the event that the current PC is destroyed processing the workload, the testing of the plan must require installing backup programs and data on the replacement PC, and ensuring the replacement PC functions as intended.

5.2 Security Incident Identification, Reporting, and Resolution

5.2.1 Background

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 (5.4.1 References, Laws and Regulations).
    - 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.

5.2.1.1 Incident Reporting Process

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) within 15 minutes of the occurrence.

NOTE

When reporting suspicious phone calls or emails, please follow the reporting procedures outlined on OIS' Social Engineering Resources page.

5.2.1.2 Reporting Loss or Theft of Personally Identifiable Information (PII)

Policy and instructions regarding the loss of Personally Identifiable Information (PII) are located in Administrative Instructions Manual System (AIMS) General Administration Manual (GAM) 15.01 ff.

5.2.2 SSA Security Response Team (SSASRT)

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

5.2.2.1 Additional Incident Response Information

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 Incident Reporting definition on the OIS homepage.

The following are examples of incidents and attacks:

- Denial of Service (DoS).
- Unauthorized control or modification of webpages.
- Vulnerability scanning.
- Password cracking.
- Network sniffing.
- Social engineering.
- Session hijacking.
- Address spoofing.

- Systems Intrusions.
- Malicious Code (virus, worm, or Trojan horse).
- Email bombardment (spamming).
- Unauthorized change in system configuration.
- Discovery of an unknown "hidden file".
- Repeated attempts to access SSA's systems (hacking).
- Stranger's attempt to learn Personal Identification Numbers (PINs), and passwords under false pretexts (Social Engineering).

NOTE

See the link to Virus Alerts on the OIS homepage, on preventing and identifying malicious code incidents.

5.2.2.2 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 Section 5.3.4 of this handbook, and in the Program Operating Manual System 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.

5.2.3 PII Loss – Procedures for All Employees

The PII Portal is the definitive source of information concerning PII information and loss reporting..

5.3 Criminal Violations and Fraud Policy

5.3.1 Background

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 the Programs Operations Manual System (POMS) (see POMS in References).

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

5.3.1.1 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).

5.3.1.2 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 30 days 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).

5.3.1.3 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).

5.3.1.4 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.

5.3.1.5 Request for Assistance by SSA OIG

The 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.

5.3.1.6 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.

5.3.1.7 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 comply with 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.

5.3.1.8 Detecting Violations

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

- **Integrity Reviews** – These include the (b) (7)(E) [redacted] These reviews identify transactions, which have a high risk for potential fraud.
- **Security Alerts** – Security alerts are system-generated notifications for many transactions, which are at high risk for fraud and abuse. These alerts bring potentially fraudulent transactions to the attention of CSOs and Regional Security Officers (RSOs).
- (b) (7)(E) [redacted] and collects information based on transactions entered by individual systems users. It provides information to support the investigation of individuals suspected of fraud.

- (b) (7)(E), in the OIS under the DCS, specializes in (b) (7)(E), and performing (b) (7)(E)

5.3.1.9 Security Administration Reports

SSA has developed the online (b) (7)(E)) derived from SSA's (b) (7)(E) security system to allow Information Security Officers (ISOs), ISO alternates, and other management designees to access, review and take action on Security Administration reports. You (the employee) can obtain access by submitting a request through the (b) (7)(E) section of the (b) (7)(E) website. The following reports are currently available:

- (b) (7)(E)
-
-
-
    - ISOs / CSOs must ensure that these reports are reviewed and any necessary action taken as described in (ISO 4.13 (b) (7)(E) Administration Reports).

5.4 References

5.4.1 Laws and Regulations

- Computer Fraud and Abuse Act of 1986, P.L. 99-474, 18 U.S.C. 1030.

- Computer Security Act of 1987 (Public Law 100-235) (H.R. 145) January 1988
- E-Government Act of 2002 (Public Law 107–347) (H.R. 2458/S. 803) December 17, 2002
- E-Government Act of 2002, Title III, Federal Information Security Management Act (FISMA)
- Government Information Security Reform Act, P.L. 106-398, Title X (2000)
- Privacy Act of 1974, P.L. 93-579, 5 U.S.C. §552a (1974)
- Freedom of Information Act, P.L. 90-23, 5 U.S.C. §552 (1967)
- Freedom of Information Act, P.L. 93-502, Amendments 1974

5.4.1.1 SSA

- POMS GN 03312.000, Disclosure for Law Enforcement Purposes
- POMS GN 03312.001, Disclosure Without Consent – Law Enforcement
- E8551- Reporting Form for Programmatic Fraud
- Office of Inspector General (OIG)
- Office of Labor and Management Relations – Sanctions for Unauthorized System Access
- POMS – GN 04100.000 Violations/Fraud
- GN 04111.005 Reporting Program Violations – General
- GN 04111.010 How the Field Office (FO) Reports Program Violation
- GN 04112.005 Reporting Employee Criminal Violations – General
- GN 04112.010 Administrative Action
- GN 04112.015 How Employees Report Employee Criminal Violations
- SSA Software Engineering Technology Manual, Part 120, *Systems Security*
- SSA Administrative Instructions Manual System
- General Administration Manual, – (ISP Section V, Contingency Planning and Incident Response)

5.4.1.2 Office of the President

- FPC 65, Federal Executive Branch Continuity of Operations (COOP)
- PDD-63, “Critical Infrastructure Protection”
- PDD-67, “Enduring Constitutional Government and Continuity of Government Operations”
- Presidential Decision Directive 63 – “Critical Infrastructure Protection”
- OMB Circular No. A-130, “Management of Federal Information Resources”, Appendix III, "Security of Federal Automated Information Systems”

5.4.1.3 OMB

- Circular A-123, “Management Accountability and Control”
- Circular A-130, “Management of Federal Information Resources”
- Circular A-130, Appendix III “Security of Federal Automated Information Systems”

5.4.1.4 NIST

- SP 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995
- SP 800-18, Rev. 1, Guide for Developing Security Plans for Information Technology Systems, Feb 2006
- SP 800-100, Information Security Handbook: A Guide for Managers, October 2006
- ITL Bulletin, "Computer Attacks, What They Are and How to Defend Against Them", May 1999
- SP 800-12, An Introduction to Computer Security: The NIST Handbook – Chapter 12, October 1995
- SP 800-61, Computer Security Incident Handling Guide, January 2004
- SP 800-100, Information Security Handbook: A Guide for Managers – Chapter 13, June 2006

5.4.1.5 DHS

- Homeland Security Presidential Directive (HSPD) 6, Integration and Use of Screening Information, September 16, 2003
- Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003

5.5 Additional Information

- Information System Contingency Plan (ISCP) template
- ISP 5.2.2: SSA Security Response Team (SSASRT)

6 Section VI: Sensitive Data Protection

Introduction: Social Security Administration (SSA) Managers and users must take appropriate action to secure and prevent improper use, altering, or destruction of SSA data. The extent of these actions must be equal to the information's sensitivity, the application's criticality, and the value of agency information or software stored on hardware or media.

Purpose: This section provides the policy governing sensitive data loss at the SSA as well as encryption. It also provides policy on how to use the SSA email and facsimile (Fax) services securely. The policies provided in this section work along with other agency policies that also affect email and Faxes. This section also provides policy related to disposal of IT equipment and paper records, Internal Revenue Service (IRS) Federal tax information, and removable media. Together, these policies ensure appropriate access to, and use of, these agency resources to accomplish the agency's mission.

Scope: The scope encompasses all Information Systems and Automated Information Systems (AISs) administered by SSA, or on behalf of SSA. This section applies to all Social Security Administration (SSA) employees, Disability Determination Service (DDS) employees, temporary staff, contractors, and other users when they act on behalf of SSA or use SSA Information Systems resources. It is important to note that, due to the unique relationship of the DDSs, supplemental regulations, and policy specific to these operating units are coordinated and distributed through SSA's Office of Disability Determinations (ODD), in the Office of Operations.

This policy addresses all SSA data, which include unstructured electronic records, metadata, and data within electronic communications, an electronic information system, in print, and archive/backup data on all forms of media as defined by the Code of Federal Regulations, Part 1236, Subpart 1236.2.

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

6.1 Data Management & Custodianship

6.1.1 Background

This policy outlines SSA internal data management requirements and security objectives throughout the data lifecycle, which includes data's creation, modification, storage, usage, sharing, and disposal. This policy also defines data and data custodianship as associated with the agency.

6.1.2 Policy

- 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 2: Access Control
- Access - Manage access to data in accordance with policies and procedures discussed within ISP Section 2: 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.

6.1.3 Security Objectives

The Federal Information Security Management Act (FISMA) framework defines three security objectives for information and information systems:

- Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]
- Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]
- Availability - Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]

6.1.4 Security Categorization

SSA data, and information derived from data, are sensitive and varies in level of sensitivity, dependent on its specific utility and the potential impact of an unauthorized disclosure. In implementing security controls, evaluate the potential impact 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.

Potential Impact	Definitions
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.

6.1.5 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 2: 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.

6.1.6 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** – At least annually, assess whether continued business need for access to data exists. If access is no longer needed, disable access to, and/or discard data.

6.1.7 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), and SSA proprietary business data.

    - Personally Identifiable Information (PII) - "PII is 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."
    - 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). More information on FTI is available via IRS Publication 1075.
    - 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.

6.1.8 Audit

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.

6.2 Removable Media and Protection from Data Loss Policy

6.2.1 Removable Media Devices

The policy areas associated with removable media devices are:

- Prohibited to connect personally owned 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 to SSA information resources. This includes connecting devices for charging them through a USB connection.
- Prohibited to store agency information on personally owned media.
- Agency personnel may accept electronic information from the public contained on removable media including but not limited to USB drives, CDs, DVDs, and floppy disks if the information is for claims processing, or other programmatic purposes provided that the following conditions are met:
  - Up-to-date automatic antivirus 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.

NOTE

If new or updated information is being returned to the customer, removable media encryption must be considered per AIMS 15.04.05.

6.2.2 Data Loss Protection

Policy for data loss prevention includes:

- ISP 6.5.1 Disposal/Donation of IT equipment 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, encrypt or protect sensitive information 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.
    - If offsite storage is not feasible, store the backup media in a locked fireproof container, in a safe place, as far away from the LAN room as possible.
    - 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 6.5.2 IT Equipment Safeguards).

6.2.3 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.

6.3 Encryption Policy

6.3.1 Background

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:

- Agency data on mobile computers / devices and removable media must be encrypted, unless the data is deemed to be non-sensitive by the SSA DC or their designee, in writing.

NOTE:

Authorized technical support personnel can use unencrypted removable media that contains non-sensitive information, without SSA DC approval, for hardware and software administration and technical support activities.

- All agency-sensitive 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).
- Files encrypted for external users require a key length of nine (9) characters.
    - The key (may also be called a password) must include both a number and a special character.
    - When delivering the key, do not physically attach the key to the media, or ship in the same package.
- Encryption-related information (such as keys) must be secured when unattended or not in use.
- It is prohibited to decrypt information you are 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 in transport for use by SSA 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).
- Encryption is generally not required for data at rest (data used locally at the site, or used at multiple sites) behind the SSA firewall.

An exclusion to this policy allows components the consent-based option of delivering unencrypted CDs "in person" or "by mail" to Number Holders and authorized representatives with the understanding that the individual receiving the CD now assumes all responsibility for the loss of any personal information.

6.3.2 Laptops

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 http://dibrla.ssahost.ba.ssa.gov/default.htm.

6.3.3 Removable Media

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, DVDs, or floppies containing sensitive information. For additional information and guidelines for using Check Point software, see Removable Media File Encryption.

6.3.4 Key Management

SSA establishes and manages cryptographic keys for required cryptography employed within agency Information Systems.

The Information System Owner (ISO) is responsible for determining the need for public key certificates, acquiring them and for the lifecycle management of keys utilized for their respective systems. The Office of Systems Operations and Hardware Engineering (OSOHE) serves as the SSA Registration Authority (RA).

6.4 Secure Electronic Mail (Email) and Facsimile (Fax) Use Policy

6.4.1 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, they are obligated to take immediate steps to deliver to the correct addressee or return to the sender. To the extent possible, they should not

read the misdirected message. Delete the misdirected message or destroy it after delivery to prevent further unauthorized access.

6.4.2 Secure Email Procedures

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 secure partners list.

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
Person/organization using @ssa.gov address	Person/organization using @ssa.gov address	Secure	Yes
Person/organization using @ssa.gov address	One of the listed secure partners	Secure	Yes
One of the listed secure partners	Person/organization using @ssa.gov address	Secure	Yes
Person/organization using @ssa.gov address	Person/organization that is not using either ssa.gov or listed as secure partner	Not Secure	No, unless data is protected by encrypted attachment
Neither ssa.gov nor secure partner	Person/organization using @ssa.gov address	Not Secure	No, unless data is protected by encrypted attachment

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.

NOTE

Special rules apply to e-mail messages containing PII that SSA sends to the Department of the Interior's National Business Center (DOI-NBC), which handles SSA payroll processing. SSA may transmit messages to the DOI-NBC that include only the employee name and last four numbers of the Social Security Number (SSN).

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

Attachment A contains for instructions on how to encrypt a file using WinZip.

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 (ISP 6.4.2, Secure Email Procedures) 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).

6.4.3 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, they must take immediate steps to ensure the message is forwarded to the correct addressee or returned to the sender. To the extent possible, they are not to read the misdirected message. The misdirected message must be destroyed to prevent further unauthorized access.

6.4.4 Email and Fax Monitoring

Various agency security policies result in users of agency IT systems or other government resources having "No Expectation of Privacy" in anything they store, send, or receive on SSA systems. This is present in the SSA Logon Security Warning banner that all users see and agree to prior to logging on to an agency system (ISP Section 2.1.1.5). 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.

6.4.5 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 the Personnel Policy Manual for policy governing how to access an employee's workstation.

6.4.6 Other Agency Policies That Apply to E-mail/Fax Use

6.4.6.1 Use of Government Equipment

Individuals using SSA email or 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).

6.4.6.2 Writing Guidelines

Although by nature, email is less formal than other forms of written communication, the same guidelines apply as those for paper communications [Quality Initiative for Commissioner's Correspondence (QUICC)].

6.4.6.3 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 Control).

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).

6.4.6.4 Records Retention Policy

SSA email system users are responsible for retaining or destroying email in compliance with SSA policy located at the Office of Publications and Logistics Management (OPLM), Office of Document Management (ODM), Center for Records Management (CRM) Intranet site.

Additional information addressing SSA e-mail retention is located at OSOHE FAQ in Electronic Messaging,

6.4.6.5 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.

6.4.6.6 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.

6.5 Disposal of IT Equipment and Paper Records Policy

This subsection covers the disposal / donation of PCs, hard drives, and other personal devices that may contain sensitive data.

6.5.1 Disposal / Donation of IT Equipment

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.

For information regarding the procedure for the donation and disposal of IT equipment, see AIMS MRM 4.31 and OFSM Property Disposal.

- Reformatting the media does not overwrite the data.
- 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).
    - When physical destruction is employed, the specific manner of destruction must be authorized.
    - Examples of physical destruction include shredding, pulverizing, and burning.

Disposal procedures are in the OSOHE IT Property Disposal Procedures.

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.

6.5.2 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

Paper Records Disposal

Individual offices / components may accomplish proper 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 shredded prior to being placed in recycle bins or bags for contractor pickup. Contracts for pulping or destruction of privacy-related information must meet standards appropriate for the material.

Instructions for disposition and destruction of records reside in SSA AIMS Material Resource Manual (MRM), Chapter 7 and Record 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.

6.6 IRS Federal Tax Information (FTI)

6.6.1 Background

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.

6.6.2 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.

6.6.3 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 http://www.irs.gov/pub/irs-pdf/p1075.pdf

Reporting Unauthorized 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 the Office of Information Security utilizing mailbox: ^IRS.Safeguards@ssa.gov . 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 inquires or questions concerning the content of this IRS FTI safeguard issues, to ^IRS.Safeguards@ssa.gov.

6.7 References

6.7.1 Laws and Regulations

- Privacy Act of 1974, (Public Law 93-579), 5 U.S.C. §552a
- E-Government Act of 2002, Title III, Federal Information Security Management Act (FISMA
- Federal Information Security Management Act of 2002 (FISMA) (Sec. 3544, (b) (2) (D) (iii)
- OMB Memo M-06-16, Protection of Sensitive Agency Information, June 23, 2006
- OMB Memo M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
- Donation of Equipment for Educational Purposes – AIMS MRM 4.31
- Disposition of Excess Personal Property – OFSM Property Disposal
- Federal Information Security Management Act of 2002 (FISMA)
- Freedom of Information Act, P.L. 90-23, 5 U.S.C. §552 (1967)
- Freedom of Information Act, P.L. 93-502, Amendments 1974
- Privacy Act of 1974, as amended (5 U.S.C. 552a)
- OMB Memo M-06-16, Protection of Sensitive Agency Information, June 23, 2006
- OMB Memo M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
- Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems
- NIST Special Publication 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- The Federal Records Act 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.
- Federal Information Resources Management Regulations (FIRMR), Chapter XII, Subchapter B, title 36 of the Code of Federal Regulations and Subtitle E, Chapter 201, Subchapter B, title 41.

6.7.2 NIST

- FIPS 140-2
- FIPS 197

6.7.3 SSA

- SSA Personnel Policy Manual, General Series, Chapter S297

- Policy on Limited use of Government Office Equipment Including Information Technology

6.7.4 IRS

- Internal Revenue Service Code 6103
- Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies

7 Section VII: Appendices

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

Social Security Administration (SSA) agency components may seek approval to deviate from the Information Security Policy (ISP) temporarily, by completing a policy waiver request. Waiver requests must be approved by a Manager, the Component Security Officer (CSO), and the Office of Information Security (OIS). The waiver request should be considered a last resort and be made only when the lack of a waiver would have a negative impact on SSA's services or infrastructure, and no other alternatives are available.

Waiver requests must specify the business or information gathering process that would be adversely affected without the waiver. Once a waiver request is submitted via the Waiver Request Form, they must be evaluated on a case-by-case basis. A risk-based determination will be made in the approval process of the waiver request. The Waiver Request Form may be reproduced locally and includes instructions for how to complete the form.

7.2 Appendix B: Roles and Responsibilities

BOOKMARKS

Deputy Commissioner for Systems / Chief Information Officer (DCS / CIO)
Chief Information Security Officer (CISO)
Office of Information Security (OIS)
Office of Systems Operations and Hardware Engineering (OSOHE)
Office of Enterprise Support , Architecture and Engineering (OESAE)
Office of Earnings, Enumeration, and Administrative Systems (OEEAS)
Office of Acquisition and Grants (OAG)
Office of the Inspector General (OIG)
Office of Audit (OA)
Office of Investigations (OI)
Office of Personnel (OPE)
Office of Systems (OS)
Office of Security and Emergency Preparedness (OSEP)
Office of Labor Management and Employee Relations (OLMER)
Office of Management and Budget (OMB)

Center Directors for Security and Integrity and Component Security Offices (CDSIs / CSOs)
Deputy Commissioners (DCs) and Agency Level Officials (ALOs)
Deputy Commissioner for Budget, Finance and Management (DCBFM)
Deputy Commissioner for Human Resources (DCHR)
Local Security Officers (LSOs)
Contracting Officer's Technical Representative (COTR)
Security Assessment and Authorization Contracting Officer's Representative (COR)
Security Authorization Manager (SAM)
Security Assessment and Authorization Contractor
Contracting Officer (CO) Requirements
Contractor Requirements (CR)
Contractors / Vendors (CV)
Government Accountability Office (GAO)
National Network Service Center (NNSC)
Project Manager / Systems Project Manager (SPM)
System Managers
SSA Security Response Team (SSASRT)
IT Support Staff
Capacity Systems Security / Lead Analyst
Technical Webmaster
Technical Infusion Board (TIB)
Content Webmaster
Data Custodian
Data Manager
Email Systems Administrator
Internet Services Manager (ISM)
Users (End Users)

DEPUTY COMMISSIONER FOR SYSTEMS / CHIEF INFORMATION OFFICER (DCS / CIO)

The Social Security Administration's (SSA) DCS / CIO has overall responsibility for the agency's Information Security Program, as required under the e-Government Act of 2002, Title III, Federal Information Security Management Act of 2002 (FISMA). The DCS / CIO are also responsible for implementation and maintenance of SSA's incident reporting process. The DCS

/ CIO prepare and send reports to the United States Computer Emergency Readiness Team (US-CERT) on security incidents.

The SSA DCS / CIO must approve any new system reportable to the Office of Management and Budget (OMB) under the FISMA law, and serves as the Designated Authorizing Authority (DAA) for the agency in the Security Assessment and Authorization (SA&A) process. The DCS / CIO is the senior agency official who authorizes Information System operation, and who explicitly accepts the risk of agency operations, agency assets, or individuals, based on the implementation of an agreed-upon set of security controls for the system. The DCS / CIO is the final signoff authority on agency Security Assessment and Authorization (SA&A) packages. The SSA DCS / CIO, with the support of the SSA Chief Information Security Officer (CISO), works closely with authorizing officials and their designated representatives to ensure that an agency-wide security program is effectively implemented. These assessments and authorizations required across the Agency are accomplished in a timely and cost-effective manner, and confirms that there is centralized reporting of all security-related activities. The SSA DCS / CIO is responsible for the agency-wide controls and their implementation as well as maintenance. In accordance with FISMA, the SSA DCS / CIO delegates this responsibility to the Senior Agency Information Security Officer (SAISO) / CISO.

CHIEF INFORMATION SECURITY OFFICER (CISO)

The CISO, located in the Office of Information Security (OIS), is the delegated responsible party with commensurate authority for the agency's Information Technology (IT) Security program, as designated by the DCS / CIO in accordance with FISMA. The CISO is also the interface with all external IT Security programs, guidelines, and organizations and provides leadership for SSA's IT Security Program, security initiatives, and operations in the e-Government and Internet environments.

The CISO administers all SSA security programs required by FISMA by developing appropriate security policies, standards, and procedures, and oversees their agency-wide implementation. The CISO manages all system monitoring activities and signs all Project Scope Agreements (PSAs) for new IT systems or processes and reviews and approves the list of the Agency's systems yearly inventory as required by FISMA.

The CISO is also responsible for developing SSA's security awareness training policy, providing information on training opportunities that meet the requirements of that policy, and oversees the implementation of that policy and program.

The CISO serves as the authorizer of the SSA systems and the SA&A packages. This involves reviewing the contents of the SA&A package, and evaluating their robustness for the system. The authorizer prepares a recommendation for the SSA DCS / CIO (the Designated Approving Authority (DAA)). The CISO develops, maintains, updates, and oversees the implementation of

INFORMATION SECURITY POLICY (ISP)

IT Security policy and programs for the agency and for the SA&A process on behalf of the SSA DCS / CIO.

Additional responsibilities of the CISO include:

- Establishes, maintains and oversees the SSA Critical Infrastructure Protection program and included plans and activities.
- Oversees agency-wide IT security safeguards, and implements and monitors security controls established to protect the confidentiality, integrity, and availability of SSA's systems, data, and IT assets deemed critical to SSA's mission.
- Interprets regulations and legislation affecting IT security, provides policy requirements and program direction for all facets of IT security, and coordinates efforts of component and regional security personnel.
- Establishes security level designations (jointly with the Security Authorization Manager (SAM) for the system) for all major systems, coordinates the SA&A of SSA's General Support Systems (GSSs) and Major Applications (MAs).
- Ensures consideration of new technologies and plans for the continued operation of SSA's systems that support critical agency workloads in any emergency.
- Defines, and manages the overall SSA Systems Security Assessment and Authorization Program effort, and identifies and nominates systems for inclusion in the Program.
- Ensures security documentation requirements applicable for each Assessment and Authorization effort are in compliance with Federal policies, regulations, and standards, and authorizes (as the authorizing authority) that the security requirements of each SSA system are being met, or must be met.
- Guides and oversees SSA-wide security awareness and training programs for management and employees on the IT security program.
- Sets policy for developing and implementing security requirements and safeguards for SSA's state information exchange program.
- Leads, and coordinates enterprise related security policy.
- Works with other components to enhance security functionality.
- Except for those functions retained by the CISO, as the SSA's SAISO, delegates all other FISMA IT Security Program functions to the Systems, Operations, Business Functions Directorates, and components. These organizations must ensure compliance with all FISMA, OMB, Federal Standards, and SSA IT Security Policies and Standards and must keep the DCS / OIS advised of all IT Security activities, issues, and accomplishments.

OFFICE OF INFORMATION SECURITY (OIS)

The OIS supports the DCS / CIO and CISO in carrying out the Information Security responsibilities required by FISMA and other related laws, regulations, and standards. The OIS is managed by the SSA CISO, who is directly responsible to the DCS / CIO for developing, and maintaining an agency Information Security Program and its associated agency-wide functions.

INFORMATION SECURITY POLICY (ISP)

FISMA requires the Agency DCS / CIO (through delegation by the agency Head) to, among other tasks, establish an agency-wide Information Security Program. To carry out those responsibilities, the DCS / CIO delegates the day-to-day responsibilities of directing and coordinating the agency Information Security Program to the agency CISO.

Other tasks under the OIS's auspices are:

- Ensures safeguards comply with Federal law, regulations and other mandates to protect the confidentiality, integrity, and availability of SSA information and systems (including appropriate risk designations for personnel positions) are part of SSA's Information Security Program.
- Supports the CISO with the development and maintenance of the agency IT Systems Inventory. OIS also works with other offices and components in supporting the agency Inventory by assisting in the determination of whether new systems processes are Major IT Systems or Supporting Subsystems of existing Major IT Systems.
- Provides oversight, guidance, advice, and assistance to Managers, System Owners (SOs), Security Officers (SOs), and IT security staff on matters involving SSA's Information Security Program and agency-wide functions.
- Directs the Control and Audit Test Facility (CATF) under OESAE, which specializes in conducting special studies, and preparing ad hoc reports that identify deviations from normal case processing, and conducts investigative studies for specific or targeted anti-fraud initiatives.

The OIS is responsible for providing IT security training for the agency. OIS is responsible for ensuring that Information Security-related training courses are available for every job series, by bringing in-house contractor training courses, or providing licenses for USA Learning. OIS coordinates with the SSA Office of Training and the Office of Systems Training component, to ensure a wide variety of training opportunities are available.

Under the DCS / CIO, OIS is an integral part of SSA's security program and delegated responsibilities include:

- Addresses the fundamental tenets of IT security, including:
    - Risk management.
    - Access controls.
    - Monitoring and enforcement.
    - Personnel training and awareness.
    - Continuity of operations, in conjunction with the Office of Facilities Management's (OFM) Continuity of Operations Plan (COOP).
- Consults on the development, publishing, and implementation of security requirements, procedures, and guidelines in support of security policies established by the SSA CISO.
- Issues policy and guidelines for the development of contingency plans as an integral part of the overall Systems Security Program. The director of OIS chairs the Agency's

Critical Infrastructure Protection (CIP) Steering Committee. The committee's chief mission is to bring the agency into compliance with Department of Homeland Security (DHS) and National Institute of Standards and Technology (NIST) requirements and guidelines for ensuring that SSA personnel, critical IT infrastructure, and physical IT facilities are sufficiently protected and recoverable in the event of a catastrophe.

- Administers and authorizes changes to the (b) (7)(E) (application) profile access authorization matrix with the responsibility for implementing and ensuring compliance with systems access policies and procedures. OIS approves any changes recommended by other staffs and implements security access policies and procedures through the Information Security Policy and the Information Security Officer (ISO) Manual.
- Oversees the establishment of the Center Directors for Security and Integrity (CDSI) and Component Security Officers (CSOs) on (b) (7)(E) and provides them with security administration authorities.
- Provides guidance and advice to SOs in matters regarding systems access controls including establishing user Identification (ID), maintaining access transaction activity, and periodically reviewing access controls.
- Serves as SO when the designated Regional and component security staffs are not available to perform security administration for their users.
- Develops and disseminates training and awareness materials in coordination with the CISO.
- Provides security, audit, and integrity review requirements for all major SSA systems, and consultation, and support for a variety of agency initiatives including management of SSA's fraud monitoring and reporting activities.
- Resolves security and policy issues regarding Risk Management, and revises / updates SSA Risk Management guidance as appropriate.
- Ensures the (b) (7)(E) and integrity review systems meet the Agency's audit and integrity review requirements by:

    - Determining which employee entries must be audited
    - Determining who should have access to (b) (7)(E)
    - Maintaining the (b) (7)(E) User Manual.

- Monitors policy conformance and assesses and adjudicates requests for exceptions to SSA's IT security policy; in these policy functions, works in conjunction with all agency components, particularly DCS / CIO and CISO.
- Approves exception requests for contractors, vendors, and the Office of Inspector General (OIG), and collaborates with the Office of Systems Hardware on all requests for permanent setting changes that OIS determines to have global impact on the SSA operating enterprise.
- Ensures, along with CISO, that SSA follows the most current NIST guidelines.
- Coordinates the agency's reporting responsibilities in compliance with FISMA.
- Coordinates with the SSA Office of Training and the Office of Systems Training component, to ensure a wide variety of training opportunities are available.

- Acts as SO when the CDSI and CSOs are not available to perform security administration for their users.
- Ensures training courses are available by bringing in-house contractor training courses, or providing licenses for USA Learning.

OFFICE OF SYSTEMS OPERATIONS AND HARDWARE ENGINEERING (OSOHE)

OSOHE is responsible for maintaining the Disaster and Recovery Plan (DRP), and Emergency Response Procedure (ERP). The DRP is the agency's contingency plan for responding to major outages affecting critical systems resources at the National Computer Center (NCC). OSOHE is also responsible for carrying out periodic testing of the plan, including the move to the "hot site", setup, and readying the system for execution.

The OSOHE staff oversees the administration and maintenance of the TOP SECRET software on all central processing units at SSA Headquarters. TOP SECRET controls all users' access to production, training, and test systems.

OSOHE also:

- Procures, installs, and maintains SSA's Local Access Network (LAN) environment in compliance with agency security policy. This (1) includes contingency planning, and backup hardware to support all critical functions, and (2) develops, procures, or otherwise makes available training specific to the use and management of SSA LANs.
- Adjudicates all requests for setting exceptions including completion of the Requests for Exception Decision form. OSOHE performs an evaluation, prepares a decision within approximately two weeks of receipt of the request, and sends a copy of the decision to the Center Director for Security and Integrity / Component Security Officer (CDSI / CSO) and to the Office of Electronic Services and Technology (OEST. OSOHE is responsible for responding to follow-up requests from CDSI / CSOs, and is the repository for all original support documentation on the final disposition of exception requests.
- Releases all application software as well as performs the integration testing of all hardware and software that is developed or procured for the LAN environment. OSOHE must be responsible for all software maintenance and release management. OSOHE must also be responsible for installation and update of LAN operating systems software, software fixes and new software releases.
- Manages connectivity of devices and users in mitigating security risk to the network.

OFFICE OF ENTERPRISE SUPPORT, ARCHITECTURE AND ENGINEERING (OESAE)

The OESAE supports the CISO's FISMA responsibility by maintaining and updating the agency's Systems Inventory process and security architecture. OESAE works with agency Business and Systems Project Owners in determining the impact of the new system and where it must reside under the agency Infrastructure. This includes working with OIS and the CISO to

determine if the process will be a new reportable Major IT System or if it must be a supporting Subsystem of an existing Major IT System.

OESAE, under the Deputy Commissioner for Systems:

- Identifies the strategic Information Technology (IT) resources needed to support SSA business processes and operations, and develops the transition processes for researching, demonstrating, and implementing new technologies in response to the Agency's strategic vision.
- Develops policies and procedures to implement the Section 508 legislation Agency-wide.
- Directs the design, development, and maintenance of SSA's IT architecture program, and directs SSA's database integration.
- Directs a comprehensive IT architecture program to modernize the Agency's infrastructure and establishes enterprise policies for the management of all hardware and software.

OFFICE OF EARNINGS, ENUMERATION, AND ADMINISTRATIVE SYSTEMS (OEEAS)

The OEEAS provides coordination of audit requirement development with OIS and within Office of Systems.

OFFICE OF ACQUISITION AND GRANTS (OAG)

The OAG is the procurement office at SSA, and is responsible for awarding, and administering SSA contracts, orders, and grants, and for issuing SSA's acquisition policies and procedures. The OAG Website provides information to assist SSA components with acquisition planning, acquisition policy, and other general information.

OFFICE OF THE INSPECTOR GENERAL (OIG)

The OIG is responsible for investigating allegations of criminal violations, and, if appropriate, preparing cases for criminal prosecution, civil suit, and / or administrative sanction.

OFFICE OF AUDIT (OA)

The Office of Audit (OA), within the OIG, conducts comprehensive financial and performance audits of SSA's programs and operations. In its reports, OA makes recommendations to help SSA achieve program objectives effectively and efficiently. Financial audits, required by the Chief Financial Officers Act of 1990, assess whether SSA's financial statements fairly present the agency's financial position, results of operations, and cash flow. Performance audits review the efficiency and effectiveness of SSA's programs. The OA also conducts short-term management and program evaluations focused on issues of concern to SSA, Congress, and the general public.

OFFICE OF INVESTIGATIONS (OI)

The Office of Investigations (OI), within the OIG, conducts and coordinates investigative activity related to fraud, waste, abuse, and mismanagement of SSA programs, and operations, in accordance with the Quality Standards for Investigations published by the President's Council on Integrity and Efficiency, the SSA OIG Special Agent Handbook, and other applicable laws, policies, and regulations. These activities include wrongdoing by applicants, beneficiaries, contractors, physicians, interpreters, representative payees, third parties, and SSA employees. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

OFFICE OF PERSONNEL (OPE)

The Office of Personnel (OPE), under the Deputy Commissioner for Human Resources, Center for Personnel Security and Project Management (CPSPM):

- Formulates SSA's personnel security and suitability policies and procedures, as well as the day-to-day operation of the personnel and security suitability programs.
- Initiates required personnel background investigations through the Office of Personnel Management, makes suitability and security clearance determinations consistent with agency policy, procedures, and grants, or withholds security clearance for employees to occupy a sensitive position.
- Concurs with the Contracting Officer's Representative (COR) and line management's sensitivity / risk level determination for each contractor position (ISP 1.8 Personnel Security and Suitability Program); for personnel security clauses and procedures for security / suitability checks for contractor personnel, see the Office of Acquisitions and Grants (OAG) Webpage
- Issues removal letters for contractor employees who receive an unsatisfactory determination and forwards a copy to the Contract Officer (CO) and COR.

OFFICE OF SYSTEMS (OS)

The Office of Systems (OS), under the Deputy Commissioner for Systems, works with OIS, and the CISO to resolve system access and audit problems as they occur, and develops new audit requirements as part of the Systems Development Life Cycle (SDLC). As functionality is added to an application system, OIS examines that functionality to determine whether or not audit changes are required based on audit policies. If audit changes are required, OIS communicates these changes to OS for inclusion in the formal systems requirements package for the upcoming application release. OS is also responsible for:

- Working with OIS to determine the best way to meet audit requirements and developing new audit programs based on the requirements;
- Maintaining the (b) (7)(E) and resolving audit problems as they occur

- Implementing access control requirements and maintaining the access control system (b) (7)(E)
- Developing security controls in conjunction with the development of application functionality, and evaluating the risks to agency data and functions created by systems development projects, in order to ensure the implementation of all required controls;
- Working with other components, including OIS and the CISO, to determine the best methods for implementing security controls;
- Validating new systems functionality to ensure that security controls are effective, and recommending alternative control methods if a needed control cannot be implemented;
- Ensuring proper documentation of lifecycle control requirements in the official agency lifecycle procedures in order to provide the level of control that the CISO requires;
- Working with OS Component Security Officers (CSOs), OIS, and CISO to evaluate the risks to agency data and functions created by systems development projects;
- Developing a Validation Plan that includes validating security controls in order to ensure that security controls are effective, and recommending alternative control methods if a needed control cannot be implemented;
- Maintaining the Project Resources Guide (PRIDE) Website (Systems Process Improvement staff) to document SSA's official procedures for the SDLC;
- Ensuring that lifecycle control requirements are properly documented in the official agency lifecycle procedures;
- Working with OS CSOs and the CISO to evaluate the risks to agency data and functions created by systems development projects, and to ensure that all required controls are implemented;
- Developing requirements documentation that must provide the level of control required by the CISO;
- Maintaining the access control system; and
- Reporting security problems to the CISO for necessary action.

OFFICE OF SECURITY AND EMERGENCY PREPAREDNESS (OSEP)

The Office of Security and Emergency Preparedness (OSEP) within the Office of Budget, Finance, Quality, and Management has overall responsibility for formulating, and directing the agency's physical and protective security program. The Office of Protective Security Services (OPSS) manages activities related to the development of policies and standards governing the implementation of physical security criteria, and related equipment for offices, and facilities for which OSEP is responsible. OSEP also:

- Establishes agency policy to ensure the safety and security of our employees, visitors, buildings, and equipment;
- Executes the agency's nationwide security program,
- Leads the agency's policy, implementation, and management of the Personal Identity Verification (PIV) and credentialing process, which includes all steps from establishing the identity of individuals to issuing and using the credentials;

- Maintains an acute awareness and knowledge of state-of-the-art security and innovative technologies and practices;
- Reacts promptly and decisively in response to emergency situations and requests for assistance‘
- Develops preventive measures to ensure the safety and well-being of agency employees, visitors, and property;
- Provides oversight, consultation, and assessments on physical security factors, including response to incidents, security alarm systems, building access, security risks, and SO duties
- Provides training to ensure the safety and security of SSA employees, visitors, and property.

Employees should contact their respective guard control center to report incidents (e.g. Theft, vandalism, unattended packages). Please refer to the building control center phone numbers below:

- Main Complex* - Altmeyer Control Center (b) (6) , Robert M. Ball, Annex, East, West, and Supply Buildings.
- Security West - Control Center (b) (6) .
- National Computer Center - Emergency Command Control Center (b) (6)
- Outlying Buildings - Federal Protective Service (Regional Control Center) (b) (6) (b) (6)

OFFICE OF LABOR MANAGEMENT AND EMPLOYEE RELATIONS (OLMER)

The OLMER, under the Deputy Commissioner for Human Resources (DCHR):

- Provides overall management of the SSA-wide program of labor management, and employee relations.
- Develops, and evaluates programs including policy regarding Sanctions for Unauthorized Systems Access.

OFFICE OF MANAGEMENT AND BUDGET (OMB)

The OMB, under the Executive Office of the President, assists the President in the development and execution of his policies and programs as follows:

- Assists in the development, and resolution of budget, policy, legislative, regulatory, procurement, e-Government, and management issues on behalf of the President.
- Develops and provides direction on the implementation of financial management policies and systems.
- Coordinates efforts to improve Federal procurement law, policies, and practices.

- Oversees Federal regulations, information requirements, and develops policies to improve government statistics, and information management.
- Issues instructions and information to Federal agencies through OMB Circulars.

CENTER DIRECTORS FOR SECURITY AND INTEGRITY AND COMPONENT SECURITY OFFICERS (CDSIs / CSOs)

CDSIs / CSOs) are responsible for advising and working with management to ensure the implementation of Federal laws and directives and SSA security policy within their area of jurisdiction. They are charged with regionally implementing, and enforcing National and Regional security directives. They may add, and apply additional requirements or procedures to such laws, requirements, and policies, as appropriate, to make them more meaningful or rigorous in their jurisdiction. CDSIs are the first Point of Contact (POC) on Regional security issues.

CDSIs / CSOs, or their designated alternates are responsible for establishing and deactivating system users and for maintaining security access controls. CDSIs /CSOs designate Local Security Officers (LSOs) to assist in this process. Center Directors should request access to the ATS for members of their staff from OIS.

The CDSIs and CSOs have the following additional responsibilities:

- Develops any additional policies needed in their Region / component because of local conditions, recommending training opportunities to meet those requirements, and reviewing the adequacy of employee training within their Region / component.
- Oversees that email and facsimile (Fax) policies are implemented within their areas of jurisdiction.
- Reports incidents for their respective components and, where appropriate, works with the SSA Security Response Team (SSASRT) and / or Office of Protective Security Services (OPSS) to resolve incidents.

CSOs ensure that SSA's policies and procedures are followed within the organization. They develop, implement, and manage the security program within their component, and must be familiar with SSA security policy and procedures. CSOs located within Central Office and the CDSIs located in the Regions are both an integral part of SSA's network of security administrators.

The CSO provides guidance and assists the SSA Security Authorization Manager (SAM) throughout the Security Authorization and Assessment (SA&A) process. The SSA CSO may also conduct a security risk assessment of the system or assist any contractor staffs who are performing a risk assessment or developing any other security related documentation or evaluation of the system.

SSA has defined Security Officer (SO) responsibilities to implement and maintain the initiatives outlined in the Federal Managers' Financial Integrity Act of 1982 (FMFIA), FISMA, and various OMB circulars and circular appendices relating to internal controls in Federal agencies. See the

Information Security Officer (ISO) Manual for more detailed descriptions of CSO security duties.

DEPUTY COMMISSIONERS (DCS) AND AGENCY LEVEL OFFICIALS (ALOS)

The DCs and ALOs are responsible for assisting in the development of contingency plans for automated systems affecting their business functions. Their major role is to determine which parts of automated processes, if any, can revert to manual processing, determine the priority of business functions, the length of time these functions can operate without automated support, as well as establish contingency plans, and critical priorities for automated processing. Specifically, they:

- Ensure designation of a security level (as defined in Security Level Designations) for each Automated Information System (AIS) within their jurisdiction.
- Provide final approval for designating a system, as an OMB Circular No. A-130 "sensitive system".
- Ensure that each System Manager has designated specific responsibilities for each sensitive system, as described in this policy.
- Ensure that required security safeguards are in place for all sensitive systems, with the understanding that non-compliant devices may be restricted from network connectivity.
- Ensure that their systems meet, or will meet, their security requirements.
- Develop and approve, for a system with security deficiencies, a corrective action plan that ensures implementation of corrective action in a timely manner via the Documented Acceptable Risk submission process .
- Ensure that each sensitive system has an up-to-date security authorization and security plan.

The DCs approve the SSA Major IT Systems operation under a Shared Authority Agreement. They also approve the development of new systems processes that allow the agency to complete its mission.

DEPUTY COMMISSIONER FOR BUDGET, FINANCE AND MANAGEMENT (DCBFM)

The Deputy Commissioner for Budget, Finance and Management (DCBFM) has overall responsibility for SSA's monitoring of compliance with the Information Systems Security policy.

DEPUTY COMMISSIONER FOR HUMAN RESOURCES (DCHR)

The DCHR is responsible for developing policy and maintaining the SSA personnel security and suitability program. The forms used in connection with this program may be found on the Office of Personnel intranet site at http://personnel.ba.ssa.gov/ope/

INFORMATION SECURITY POLICY (ISP)

Personnel security clauses and procedures for security / suitability checks for contractor personnel, besides the initial issuance, may be found on the OAG Web page. The initial issuance may be found on the OAG website.

The DCHR, through the OPE, CPSPM is responsible for the day-to-day operation of the personnel, and security suitability programs. The OPE / CPSPM:

- Formulates SSA personnel security and suitability policies and procedures.
- Concurs with line management's sensitivity / risk level determination for each contractor position.
- Initiates required personnel background investigations through the Office of Personnel Management (OPM).
- Makes suitability and security clearance determinations consistent with agency policy, and procedures.
- Grants, or withholds security clearance to occupy a sensitive position.
- Issues removal letters for contractor employees who receive an unsatisfactory determination, and forwards a copy to the CO and COR.

LOCAL SECURITY OFFICERS (LSOS)

LSOs are charged with implementing IT Security policies and maintaining security access controls within their area of responsibility.

CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (COTR)

The COTR works very closely with the CO in developing and administering contracts and grants. For detailed duties, see the COTR Resource page.

COTRs perform the following:

- Represents the program office and ensures that program requirements are clearly defined and that the contractor meets them. He / she must ensure that competitive vendors are solicited, evaluated, and selected, and that the service, and equipment costs are reasonable. COTRs establish, and monitor quality standards, and delivery requirements. While the contract is in force, COTRs ensure compliance with all contract provisions and applicable laws and report any deviations to the CO.
- Ensures that the Statement of Work (SOW) adequately outlines the SSA Security and AIS requirements, including safeguarding Internal Revenue Service (IRS) Tax Return information, as part of the requirements analysis.
- Ensures the SOW includes in all relevant security statements
- Forwards SOWs to the DCS / CIO's office for review / approval, if a Request for Proposal (RFP) involves a General Support System, a Major Application System, or if it

exceeds the dollar threshold specified in the IT Capital Planning and Investment Control (CPIC) document.

- Contacts and coordinates with the CSO / CDSI regarding required off-site facility inspections.
- Coordinates with the SO to ensure contractor personnel are fully informed of their security responsibilities and are aware of their responsibilities for protecting sensitive information as specified by the security requirements in the SOW.
- Determines, in conjunction with the applicable line management, the sensitivity / risk levels for contractor positions, and forwards requests for contractor access to SSA systems.
- Manages the contract and day-to-day contact with the contractor and monitors, on an ongoing basis, contractor adherence to the security provisions.
- Conducts preliminary security assessment and analysis of security requirements, including whether Federal Tax Information is involved, as part of the requirements analysis.
- Briefs contractors, in coordination with the CDSI / CSO, on SSA security requirements regarding confidentiality, disclosure, and protection of information entrusted to them.
- Ensures that the contractor signs the SSA Awareness Contractor Personnel Security Certification (PSC) (SSA-222) form prior to receiving access to Agency systems and maintains completed PSC forms.
- Ensures that all contractor personnel sign the SSA Awareness Contractor Personnel Security Certification (SSA-222) form and if appropriate the ISP - Non-Disclosure Agreement for removal of SSA sensitive information form.
- Coordinates with the SO to ensure that personnel suitability background investigations are performed for certain contractor personnel (ISP 1.8 Personnel Security and Suitability Program).
- Ensures on-site inspections and/or testing of the Offeror's computer security safeguards.
- Evaluates the security plan, and monitors contractor adherence to agency security policies.
- Completes the exit process with the contractor for each contract employee separated from performing on the contract, or all contract employees at the end of the contract, to ensure that he / she has returned all building credentials, badges, sensitive materials, etc., to SSA upon completion or termination of the contract, and makes the individual inactive in the (b) (7)(E) active contractor database; also reviews a contract employee's reason for resignation or termination to determine if further SSA action is necessary.
- Ensures all grantee / contractor personnel receive appropriate security training commensurate with their responsibilities.
- Ensures that contractors are only given temporary access to the Agency's systems as needed. Detailed information is available on the ISP, 2.1 Information Systems Logical Access Control Policy

- Ensures contractors are aware that unauthorized access of agency information for personal gain (including, but not limited to monetary gain), or with malicious intent is prohibited.
- Ensures that all contractors abide by the security policies contained in the SSA's Information Security Policy security policies.
- Ensures that unauthorized disclosure of information is prohibited. This information includes:

    - SSA programmatic and sensitive information.
    - IRS Tax Return information.

- Ensures that security is maintained at the appropriate level in compliance with SSA security policies.
- Ensures that systems are isolated prior to connecting to SSA systems.
- Notifies the CO and appropriate CSO when personnel are no longer working on the contract, are arrested, or charged with a crime during the term of the contract / grant.
- Notifies the SO and the OIS when to terminate contractor access because of end of task, change of duty, resignation, termination, etc.
- Reports contractor non-compliance to the CO for necessary action.

SECURITY ASSESSMENT AND AUTHORIZATION CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The SA&A COR oversees the SA&A contract and the contractor activities. These activities include plans the schedule of tasks to be done, writes the contract statement of work (SOW), holds appropriate meetings with contractor and SSA staff, and performs other general COR duties such as ensuring building and systems access, as needed.

SECURITY AUTHORIZATION MANAGER (SAM)

The SSA SAM is responsible for writing and maintaining the security plan for the system. It is imperative that the plan is current so that an accurate picture of the system is always available. To ensure accuracy, the Security Plan must be updated yearly or as major changes occur. The SAM evaluates the security controls appropriate for the system. Assistance for this task may be provided by the SSA CSO, the CISO, or appropriate contractor staff. The SAM is responsible for notifying the CISO if a major change occurs in the system that would warrant a new SA&A being done on the system. A determination regarding the need for a new SA&A is jointly made by the SAM and the CISO. Examples of a major change are:

- Installation of a new or upgraded operating system, middleware component, or software application.
- Modifications to systems ports, protocols or services.
- Installation of a new, or upgraded hardware platform, or firmware component.

- Modifications to cryptographic modules, or services.

Changes in laws, directives, policies, or regulations, while not always directly related to the Information System, can also potentially affect the security of the system, and trigger a re-authorization action. The SAM assembles the SA&A package with the assistance of the SSA contractor staff. The SAM Certification and Accreditation (C&A) Manager writes the requesting letter to the SSA DCS / CIO, asking that the system be certified and accredited. The SAM is also responsible for obtaining all DC-level signatures, as appropriate.

The SAM is responsible for maintaining the SA&A package and the full copy of SA&A task documents prepared by SSA / OIS staff or the SSA / OIS SA&A contractor. As these documents are sensitive, they should be maintained by placing in a locked file cabinet or desk. Electronic and / or paper copies of these documents should be distributed to the partner DCs, as appropriate. Access should be restricted and SSA / OIS staff should be contacted regarding questions about access. In the SSA / OIS SA&A process, the SAM must be a General Schedule- GS) 15 or higher.

SECURITY ASSESSMENT AND AUTHORIZATION CONTRACTOR

SSA SA&A contractors are responsible for completing all SA&A tasks that are detailed in the contract with SSA and assists the SAM in assembling the SA&A package.

CONTRACTING OFFICER (CO) REQUIREMENTS

The term CO also includes the Grants Officer in case grants.

- Ensure that all relevant security statements and contract clauses are included in all solicitation and contract documents.
- Sign the contract on behalf of the Agency and bear legal responsibility for the contract.
- Take action to terminate or change contractual commitments on behalf of the agency.

CONTRACTOR REQUIREMENTS (CR)

- Contractor personnel must abide by all security clauses in the contract.
- Contractor personnel must protect all application systems, software packages and personal / sensitive data including Federal Tax Information, trade secrets, and other SSA AIS assets, against destruction, loss, or misuse.
- Contractor personnel must adhere to SSA security policies and guidelines.
- Contractor personnel are subject to personnel suitability background investigations appropriate to designated sensitivity levels, as specified in (ISP 2.3 Personnel Security and Suitability Program) for AIS-related positions.
- In the event contractor personnel performing on a contract either leaves the company, are removed from the project, or are arrested or charged with a crime during the term of a

contract, the contractor must notify the COR and the Protective Security Officer immediately. In the notification, the contractor must provide the name and Social Security Number (SSN) of the contactor's personnel, the type of charge(s), the court date, and, if available, the disposition of the charges(s).

- Contractor personnel must sign an ISP: Non-Disclosure Agreement whenever they have access to sensitive information.
- Contractor personnel must sign an SSA Awareness Contractor Personnel Security Certification (SSA-222) form
- SSA reserves the right to inspect the facility if the contract involves performing work or storing information offsite.
- Contractors must provide offsite network diagrams to SSA upon request
- Contractor personnel are subject to prosecution under Federal Tax Information Sections 6103, 7213, 7213A and 7431 of the IRS Code.
- Contractor personnel must delete any residual data from the temporary and other locations after the session is terminated from the SSA connection.
- Contractor personnel accessing SSA systems must use virus free systems.
- The COR must be involved in all aspects of the acquisition process. This includes planning, proposal evaluation, source selection, technical direction, and contract administration.

CONTRACTORS / VENDORS

- Present a detailed outline of their security program in their proposals;
- Adhere to all contract clauses pertaining to Privacy or Security Safeguards, Federal Acquisition Regulation (FAR) 52.239-1, as stated in contract clauses;
- Review the contract clauses to ensure that the contract accurately reflects government property required to accomplish the scope of work, and at the end of the contract conduct a final inventory;
- Comply with all building access requirements for their personnel and subcontractors;
- Inform the COR of incidents that may affect contract performance;
- Ensure onsite non-government issued equipment meets the minimum security standards issued by the Agency.

GOVERNMENT ACCOUNTABILITY OFFICE (GAO)

The GAO:

- Is an agency that works for Congress and the American people.
- At the request of Congress, studies the programs and expenditures of the Federal Government.
- Is referred to as the investigative arm of Congress and is independent and nonpartisan.
- Evaluates Federal programs, audits Federal expenditures, and issues legal opinions.

- When reporting its findings to Congress:

  - Recommends actions, which lead to laws, and
  - Acts to improve government operations, saving billions of dollars.

NATIONAL NETWORK SERVICE CENTER (NNSC)

The NNSC maintains the NNSC Incident Response Help Line at 1-877-697-4889 for reporting computer security incidents (ISP 5.2 Incident Reporting Process).

PROJECT MANAGER / SYSTEMS PROJECT MANAGER (PM / SPM)

The PM is the individual responsible for the entire project, and ultimately responsible to, and for the customer. At SSA this role may have more than one name, for instance, in the OS: *"Project Manager"*, *"Systems Project Manager"*, or *"Software Development Project Manager"*. The SPM is in the OS, and is responsible for overseeing project development (see Project Management Directive for a detailed description). The SPM is responsible for all technical activities for a project. In some cases, this is the same individual as the Business Project Manager (BPM). If so, the SPM subsumes the BPM's responsibilities.

The SPM:

- Establishes, and maintains an environment to facilitate interaction, coordination, support, and teamwork between the project engineering groups, between the project, and the customer or end users as appropriate, and throughout the organization.
- Establishes, and maintains detailed plans for performing software development, and testing activities based on documented requirements.
- Provides adequate resources and funding for:

  - Developing the requirements.
  - Planning, and tracking the project.
  - Designing, developing, and testing the software.
  - Performing Configuration Management (CM) activities.
  - Participating in product quality activities for products created by the team.

- Selects qualified contractors as appropriate, establishes commitments with them, and monitors their performance to ensure that they meet SSA's expectations in content, and quality.
- Manages the requirements, the changes made to the requirements, and other baseline products such as the program code.
- Negotiates commitments related to software or development activities, develops the Software Development Plan (SDP), and assigns responsibility for producing work products, completing activities, and tracking progress.

- Establishes, and maintains the integrity of the work products throughout the project's life cycle, systematically controlling changes to the system configuration.
- Incorporates Configuration Manager activities and work products into the project schedule and SDP (and related project schedule.
- Assigns responsibilities to the Project Configuration Manager (PCM).
- Ensures a configuration library system is established as a repository for the software baselines.
- Identifies the project's technical risks, analyzes the risks, and establishes mitigation plans to eliminate / reduce them.
- Ensures that documented policies, procedures, and standards are followed and that quality products are built.
- Provides input to Quality Assurance (QA) planning, and incorporates those activities into the SDP (or S/HAP) and related project schedule.
- Provides the person responsible for QA with access to the necessary information for a QA review.
- Ensures that the project team understands the roles, responsibilities, and authority of the person responsible for QA.
- Coordinates with person responsible for QA to resolve non-compliance issues identified during reviews.
- Coordinates with other Systems, and non-Systems components to ensure that issues are communicated to all parties.
- Coordinates and schedules meetings with involved Systems components (e.g., security, database, OSOHE, etc.);
- Negotiates with the BPM and the customer component to determine the Customer Satisfaction Indicator on Vital Signs & Observations Report (VISOR).
- Reviews the following activities with senior management and affected groups on both a periodic and an event-driven basis: requirements management, unresolved conflicts and changes to commitments, and project planning and tracking activities including status of effort, schedule, performance and risks, CM activities, and QA activities:

    - Manages the entire Construction phase of the life cycle (SPMs working on Internet projects) and are responsible for and producing the required documentation. The SPM is part of the project team during Planning and Analysis (P&A), acting as a technical advisor. The BPM delivers required P&A documentation to the SPM by the beginning of the Construction phase (may be multiple SPMs working on collaborative projects (one from the operational component(s), one from the OS).
    - Works as part of the project team during P&A (both (all) SPMs). The OS SPM may be responsible for documenting requirements and producing other project deliverables and coordinating with relevant OS components.
    - Ensures that meaningful Resource Accounting System (RAS) codes are identified for the software activities.

- Assessing the project's status and issues;

- Negotiating changes and taking corrective actions when the project is not achieving planned milestones and estimates, and
- Identifying the project's risks, analyzing the risks, and establishing mitigation plans to eliminate or reduce them, etc.

The PM is also responsible for ensuring that all security policy requirements are met. This includes meeting with the SAM of the inherent SSA Major system to determine where the developing system fits into the SSA System Architecture.

MANAGERS / SUPERVISORS

Managers / Supervisors must:

- Ensure that employees are aware of, and observe all security requirements of the data and AIS facilities they use.
- Ensure 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 the ISP Security Training and Awareness policy.
- Monitor user compliance and adherence to global and local security policies, guidelines, and procedures for proper use, and protection of data.
- Ensure enforcement of global SSA and local security policies for the overall security of the LAN facility under their purview, with the understanding that non-compliant devices may be restricted from network connectivity.
- Ensure reporting to their security officer of breaches of policy or procedure.
- Report security incidents to the NNSC and notify the CSO or CDSI.
- Ensure that their employees understand (1) security incident reporting procedures and (2) security policies to protect SSA Information Systems and SSA property.
- Ensure:
    - Implementation of email and fax policies within their organizations.
    - That employees are aware of the National and local email and fax policies,
    - That email and fax systems are appropriately used.
- Notify employees when others access the employee's email or fax messages.
- Notify employees that Branch Chiefs, Field Office Managers, or above, may authorize their use of email at sites other than the employee's normal work locations, and help them obtain such authorization when necessary.
- Provide all employees with the Sanctions for Unauthorized System Access Violations document, and ensure that the employees read and understand the document.
- Provide all employees with a copy of the desk reference guide: Guidance for Employees on How to Transact Social Security Business that Require Systems Access.

Management is responsible for:

- Immediately notifying their SOs when their systems users must not temporarily access the system, are transferred to another component, or leave the Agency.
- Annually ensuring that system users are aware of their responsibilities regarding access to SSA Systems as discussed in Section 5.3.1.7 Sanctions for Unauthorized System Access.
- Every three (3) years reassessing 100% of their employee's security access needs using the principles of "Need-to-Know" and "Least Privilege". Since this is a three (3) year process, a Manager may assess a partial amount of their employees each year to reach the goal of 100% at the end of three (3) years. This assessment must be documented for the administrative files by completing a form with this information.

Managers must ensure that their employees are made aware of the reporting procedures, and the security policies in place to protect SSA Information Systems, employees, and SSA property. They are responsible for reporting security incidents to the NNSC and for notifying their CSO or CDSI.

Managers must ensure that employees are aware of, and follow appropriate policy and procedures for reporting alleged criminal violations, and ensure any related sanctions are enforced.

Managers at all levels are responsible for seeing that email and fax policies are implemented within their organizations. They must ensure that employees are made aware of the National and local email and fax policies and ensure that those systems are appropriately used.

Managers at all levels are responsible for implementation of the encryption policy within their organizations. They must ensure that employees are made aware of the encryption policy, and verify that it is implemented appropriately. Managers are responsible for notifying their SO of any encryption system compromise.

Line management, with the concurrence of Center for Personnel, Security and Project Management (CPSPM), must determine the sensitivity / risk levels for AIS positions within their respective components, consistent with OPM-established regulations. Management must use sound judgment in making these decisions. Managers should refer to the SSA Position Risk Designation Checklist for assistance in determining the most appropriate risk / sensitivity level designation. They should complete and submit this checklist to CPSPM anytime a position is created or when they substantially modify the duties of an existing position. PMs / COR should remember to use CSOs as a resource for AIS-related contractor / vendor activity.

Regional / component management is responsible for ensuring that all employees within their component receive all security training required for the employee to effectively meet their security responsibilities.

Supervisors are responsible for identifying security training needs of their employees and recommending employees for the training they require. They are also responsible for ensuring that their employees are aware of security requirements, and for monitoring employee compliance with those requirements.

SYSTEM MANAGERS

System Managers are responsible for the physical and electronic security of the data and the data processing capabilities of their AISs. Generally, this is the management official for the staff that is operating and maintaining the system. Systems Managers may be Office Managers, SOs, or employees designated by management who have good technical knowledge of microcomputers.

System Managers perform the following duties:

- Certify that the sensitive systems for which their component is responsible have adequate security documentation, and maintain, and update the security plan to reflect changes to the system.
- Consult with the CSOs and system users regarding the levels of security that their data and data processing capabilities require.
- Direct, coordinate, and / or provide resources for SSA Risk Management.
- Designate the security level of LAN and computer-based applications under their purview. They establish and communicate the security safeguards required for protecting the application, the computers that run the application, and the data the application processes. They ensure that appropriate contingency plans are developed, tested, and maintained for the system.
- Develop, implement, and review security safeguards to protect the integrity, confidentiality, and availability of the sensitive system for which they have responsibility, with the understanding that non-compliant devices may be restricted from network connectivity.
- Develop a security plan for any system for which they are responsible that meets the definition of “sensitive”, as defined by the SSA Systems Security Plans and Certification Program.
- Ensure appropriate personnel have been delegated the responsibility for effecting backup operations, and that the backup copies of critical data are maintained, safeguarded, and ready for use in the event of a major disruption. Managers should make sure the plan is documented, kept up-to-date, and reviewed periodically.
- Ensure that system documentation, as prescribed in the PRIDE, is readily available.
- Ensure that staff responsible for system security know, and understand the system's control objectives and techniques.
- Ensure that they know all controls applied to their respective systems, and the status of these controls.
- Ensure adequate contingency planning:

    - Ensure that appropriate contingency plans are developed, tested, and maintained for the systems under their jurisdiction
    - Ensure that appropriate personnel have been delegated the responsibility for effecting backup operations, and that the backup copies of critical data are maintained, safeguarded, and ready for use in the event of a major disruption.

  - Ensure that the plan is documented, kept up-to-date, and periodically reviewed.

- Make decisions regarding risks acceptance, based on Risk Management activity results, in conjunction with their SOs and CISO.
- Maintain and update the security plan accordingly with changes to system.
- Manage risk for their systems and provide Risk Management training for employees.
- Take corrective actions to mitigate the risks.

SSA SECURITY RESPONSE TEAM (SRT)

The SSASRT consists of OIS and OSOHE security staff, other systems, and SO personnel, and OIG representatives who:

- Serve as technical consultants in their area of expertise.
- Respond to incidents involving computer systems, Internet and Intranet servers, and LAN Servers, including malicious code (virus, worm, or Trojan horse) and email bombardment (spamming), and alerts all end users to current threats to the system.
- Respond to reports of attempts by strangers to learn Personal Identification Numbers (PINs) and / or passwords under false pretexts (e.g., representing themselves as network troubleshooters (social engineering)).
- Investigate unauthorized changes in system configurations, or discoveries of unknown "hidden files".
- Coordinate with OSOHE in managing connectivity of devices, and users to the network when mitigating security risk to the network.

IT SUPPORT STAFF

The IT Support Staff, under the direction of the local Manager, and often working in conjunction with OSOHE, have responsibility for:

- Implementing LAN security standards at the local site.
- Ensuring each user is aware of the minimum security requirements to operate effectively within the LAN environment, with the understanding that non-compliant devices may be restricted from network connectivity.
- Ensuring all LAN configurations support the use of PINs and passwords at all times.
- Ensuring the efficient and technical operation of the SSA email systems, and maintains the integrity, and confidentiality of the email messages (IT Support Staff may not read email messages of others unless specifically directed to do so by authorized management officials).
- Reporting incidents to the NNSC, and notifying its CDSI / CSO.

IT Support staff familiar with SSA systems, may often be the first to discover a security incident.

CAPACITY / SYSTEMS SECURITY / LEAD ANALYST

- Lead Management Information Analyst
    - Provides management information requirements.
- Systems Security Analyst
    - Implements security policies and procedures, diagnoses and resolves security-related problems, promotes education and awareness of security-related issues, and performs other related tasks. Security analyst responsibilities include:
        - Designing, and developing the defined security requirements,
        - Developing the System Security Plan (SSP), and
        - Ensuring the proposed system complies with Agency security policies.
- Capacity Analyst
    - As a team leader, works with the project team to determine the service level requirements and objectives for the application.

TECHNICAL WEBMASTER

The Technical Webmaster is responsible for the links to install, configure, and manage SSA's forms, databases, and applications accessed from SSA's homepage.

TECHNOLOGY INFUSION BOARD (TIB)

- Guides and manages SSA's Technology Infusion Process (TIP) by developing, documenting, and implementing the approach for:
    - Determining candidate business / technology opportunities;
    - Prioritizing the opportunities;
    - Presenting the opportunities for approval to the Information Technology Advisory Board (ITAB);
    - Assisting in the incorporation of approved business, and technology opportunities into the agency's programmatic and business functions.
- Describes a cooperative cross-component process for conceptualizing, evaluating, and implementing uses of new technologies, or new uses of existing technologies that must facilitate SSA's ability to achieve the agency's strategic goals, and the overall objectives of Federal electronic government.

- Defines a lifecycle process for research and development of business and technology opportunities. TIB works in concert with Enterprise Architecture planning, the SSA Architecture Review Board (ARB), and other organizational processes under the auspices of the ITAB.

CONTENT WEBMASTER

The Content Webmaster is responsible for managing the content, and appearance the information on SSA's external Web server, and for coordinating the work of the Data Managers.

DATA CUSTODIAN

The Data Custodian manages access to data in accordance with access, security, and usage policies. He / she ensures that data is available only to authorized users. The Data Custodian manages data dictionaries under change-control, and assesses the broader impacts of proposed changes. The role typically involves a combination of a database administrator, a data analyst, and application-knowledgeable analyst.

DATA MANAGERS

Designated Data Managers are responsible for developing, and maintaining the content of documents that are made available on SSA's homepage.

EMAIL SYSTEMS ADMINISTRATORS (ESA)

The Email Systems Administrators are responsible for the efficient, and technical operation of the SSA email systems, and for maintaining the integrity, and confidentiality of the email messages. They are prohibited from reading others email messages unless specifically directed to do so by authorized management officials.

INTERNET SERVICES MANAGER (ISM)

The ISM is responsible for managing all aspects of SSA's Internet services including development, and approval of new Internet services, budget, and staff support.

USERS (END USERS)

Users are responsible for complying with national policy, and locally developed security access controls, and guidelines. They are responsible for protecting their PINS and passwords, and must lock or logoff their workstation / terminal prior to leaving it unattended.

INFORMATION SECURITY POLICY (ISP)

Users are responsible for adhering to all applicable policies, standards, and procedures, as well as being familiar with current security, privacy, and confidentiality practices. They *must* protect the data, processes authorized for their use, and scrupulously protect their user identification, and passwords.

All employees and other systems users are responsible for reporting security incidents. The user must immediately notify their Manager. If the Manager is not available, they must contact their SO. If the Manager and SO are not available, they must contact their Regional Automation and Security component. If all of the above are unavailable, they must contact the NNSC Incident Response Help Line at 1-877-697-4889 and select option "Report a Computer Security Incident".

SSA systems are not to be used for personal business, except as specifically permitted under the limited personal use policy. All employees are required to report suspected criminal violations using prescribed policies, and procedures.

Rules of Behavior for Users and Managers of SSA's Automated Information Resources

---

March 23, 2001

Table of Contents

1. Introduction

1.1 What are Rules of Behavior?

Rules of Behavior are a significant part of the SSA Information Security Program. They tell users and managers of SSA's Automated Information Systems (AIS) what is expected of them and how to conduct themselves while using these resources. In this way, it is easy to translate the requirements of SSA's Security Policy into daily activities.

1.2 Who is Covered by These Rules?

SSA's Rules of Behavior extend to all SSA personnel and any other persons accessing SSA Systems under formally established agreements. This includes contractor personnel as well as other external government agency users.

1.3 Why Do We Have Rules of Behavior?

The Office of Management and Budget (OMB) has established security requirements for all government agencies who use Automated Information Systems in the course of their business. The new thrust of OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, stresses management controls rather than the traditional approach of technical controls. To this end, OMB Circular A-130 requires all agencies to establish formal Rules of Behavior.

1.4 What is the Purpose of This Document?

This document, *Rules of Behavior for Users and Managers of SSA's Automated Information Resources*, describes the rules of behavior which are expected of all SSA personnel, contractors, and external users of SSA's AIS resources. It is intended to summarize rules contained in existing SSA Security Policy as described in the SSA Information Systems Security Handbook (SSH) and provide a desktop guidance document for day to day operational issues.

2. Rules of Behavior Requirements

OMB Circular A-130 requires that Rules of Behavior be written for both general support systems and major applications. These are defined as follows:

2.1 General Support Systems

OMB Circular A-130 defines a general support system as "an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications and people."

At SSA General Support Systems may include NCC mainframe operations, SSANet operations, IWS/LAN and Backbone communications capabilities as well as any contracted third party vendor products supporting the SSA infrastructure.

2.2 Major Applications

OMB Circular A-130 defines a major application as "an application that requires special attention due to the risk and magnitude of harm resulting from the loss, misuse or unauthorized access or modification of the information in the application."

At SSA such applications have been identified as *sensitive systems* and have associated security plans already in place.

2.3 Specific Rule Requirements

OMB Circular A-130 defines the specific requirements that agencies must follow in developing their Rules of Behavior.

2.3.1 Rules of Behavior must be a component of the security plan developed for each general support system and major application.
2.3.2 The level of system risk must be used as a basis for defining the rules.
2.3.3 Rules must be only as stringent as necessary to provide adequate security.
2.3.4 Rules must delineate the responsibilities and expected behavior of all individuals with access to a covered system.
2.3.5 For existing systems, the rules must correspond to any applicable technical controls present in the system.
2.3.6 Rules must address the following conditions / situations:

- work at home
- dial-in or remote access
- public access
- copyright protection and control
- official and unofficial use of government equipment
- use of system privileges

- separation of duties
- individual accountability
- information distribution
- external access to agency resources

2.3.7 Rules must include limitations / controls on:

- modifying data
- searching data bases
- divulging information.

2.3.8 Rules must be included in general support system or major application training plans.

2.3.9 Consequences of rule violations must be identified.

3. Rules of Behavior

The Information Systems Security Handbook (SSH), as well as other SSA policies and guidelines, incorporates those rules necessary to protect our systems. The rules which apply to each SSA employee have been consolidated below. In addition, recommended administrative guidelines for appropriate actions where managers are confronted with employee systems violations are to found in Sanctions for Unauthorized Systems Access Violations. 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.

Rules have been divided into two main categories; Users and Managers. Rules for Users apply to all SSA personnel or any persons accessing SSA systems in an official capacity. Rules for Managers apply specifically to personnel in managerial or supervisory positions and are in addition to the User's rules. Rules for Managers are included only in areas where a delineation is necessary.

3.1 General Rules of Behavior

Users must:

- be familiar with current information security, privacy and confidentiality practices.
- obtain written authorization before using sensitive or critical applications.
- use only systems and data for which they have authorization.
- lock or logoff their workstation/terminal prior leaving it unattended.
- act in an ethical, proficient, informed and trustworthy manner.
- protect sensitive electronic records.
- be alert to threats and vulnerabilities to their systems.

Managers must:

- monitor use of mainframes, PCs, LANs, and networked facilities to ensure compliance with national and local policies.

- ensure that employee screening for sensitive positions within their components has occurred prior to any individual being authorized to access sensitive or critical applications.

- implement, maintain and enforce systems security standards and procedures; and immediately contact their security officer whenever a systems security violation is discovered or suspected.

3.2 Official Business

Users must:

- use SSA system resources (hardware / software) consistent with SSA's policy on the personal use of government office equipment. See Appendix G for detailed information on this subject.

- protect government property from theft or misuse. SSA-owned computers are not to be removed from SSA premises unless authorized to conduct official government business.

Managers must:

- ensure that all work performed using Government resources is consistent with SSA's policy on the personal use of government office equipment .

- ensure that all personnel under their authority are aware of the rules governing the use of Government resources.

3.3 Access

Users must:

- be assigned a Personal Identification Number (PIN), when authorized, which is to be used to sign-on to designated SSA systems.

- never share their passwords.

- change passwords at specified time periods. These time periods are defined in SSA policy.

- comply with national policy and locally developed security access controls and guidelines.

- log-off the system once a session is completed to prevent unauthorized access.

- use software access controls and/or encryption to ensure that sensitive data is protected.

Managers must:

- ensure that systems users are aware of their responsibilities regarding access security.

- restrict systems access to that needed to perform assigned duties.

- implement physical access controls commensurate with the risks identified.

- ensure that SSA systems and data within their area of authority are only accessed by persons with a clear "need to know".

- ensure that access to SSA systems by employees at sites other than the normal work location is done in accordance with published security policy.

3.4 Accountability

Users must:

- use SSA systems only in the manner prescribed in published policy

- ensure that they do not attempt to override internal controls.

- abide by all established procedure related to the use of SSA systems

- report any instances of suspected fraud, abuse or misuse of SSA systems

Managers must:

- ensure that periodic reviews are performed on sensitive and critical systems for which they are responsible.

- ensure that contractor employees meet and abide by all SSA systems security requirements.

3.5 Confidentiality

Users must:

- never disclose information obtained in the performance of their duties except as described in the policy and procedures for that system.

- ensure the protection of sensitive data by exiting an application before leaving the workstation.

- ensure proper storage of sensitive data. Data stored on hard disks may be encrypted. Removable media must be locked in a secure location.

3.6 Integrity

Users must:

- never knowingly enter unauthorized, inaccurate or false information.
- obtain necessary training prior to using a system so that erroneous data will not be entered.
- scan all executable files to ensure they are virus free.
- use virus detection and scan software in accordance with policy and procedure.
- never expose critical data to conditions which may compromise the integrity of the data due to lack of adequate controls.

Managers must:

- ensure that all users have obtained adequate training on the system processes prior to system access.

3.7 Availability

Users must:

- back up systems and files on a regular basis.
- properly store removable media.
- ensure that viruses or any other disruptive events do not impact SSA systems.

Managers must:

- plan for contingencies such as disaster recovery, loss of information or disclosure of information by preparing alternate work strategies and recovery mechanisms.
- ensure that regular backups are scheduled for sensitive and critical systems.
- ensure proper storage of media, such as diskettes and tapes.

3.8 Hardware

Users must:

- use only SSA approved hardware. Employees are not permitted to bring their personally owned microcomputers or other computer resources into the workplace.

- use only SSA sanctioned procedures, hardware and software for remote access to SSA systems.

3.9 Software

Users must:

- adhere to all software licensing agreements.

- use only software that is purchased through the agency-sanctioned requisition procedures or software that has been developed, evaluated, documented and distributed in-house.

- obtain certification from the Office of Information Management before using shareware and freeware on SSA microcomputers.

- not install or use personally owned software on SSA microcomputers unless prior management approval has been obtained.

- protect copyrighted information in accordance with the conditions under which it is provided.

- not make illegal copies of software.

- not make copies of SSA purchased software for personal use.

- take measures to reasonably secure all SSA-owned software at close of business and/or anytime it is not in use.

- use only the SSA approved anti-virus software obtained through SSA licensing.

Managers must:

- ensure that corrective action is taken if such infractions are discovered.

- ensure that personal or non-government issued software is not installed on any SSA machine unless prior authorization is obtained in accordance with published policy and procedures.

3.10 Awareness and Training

Users must:

- be alert to any clues of system abuse or misuse.

- avail themselves of any opportunity to obtain further training in information and system security.

- challenge unknown personnel in their area attempting to obtain access to information or other AIS resources.

- participate in all required security training as identified by management.

Managers must:

- ensure that all individuals are appropriately trained on their security responsibilities prior to allowing them access to SSA systems.

- ensure that employees are aware of all national and local systems security policies.

- avail themselves of all appropriate security training opportunities.

3.11 Reporting

Users must:

- report security breaches to their local, regional or component security officer immediately for resolution.

- report suspected virus attacks in accordance with current SSA policy detailed in the SSH.

- report suspected violations of the Social Security Act, Privacy Act and other laws as well as SSA policies and procedures.

Managers must:

- provide an atmosphere in which personnel are comfortable in reporting suspected violations of security policy.

- take appropriate action on all reported violations and suspected violations.

- coordinate with their designated security officers on security violations reported.

3.12 Offsite Work

Users must:

- comply with all policy and procedure as outlined in the SSH for offsite work opportunities.

- not use any non-government issued hardware, software or other AIS resources in the performance of their official duties.

- not perform any non-official business functions on government owned equipment when outside the normal work environment.

3.13 Public Access

Users must:

- ensure that all information available through public access channels has been approved for public dissemination by appropriate management officials.

- ensure that they do not disclose any sensitive or inappropriate SSA information through their use of public access connections.

3.14 Internet Access

Users must:

- restrict all Internet access to access consistent with SSA's policy on the personal use of government office equipment.

- make no commitments to Internet services not approved / authorized through SSA.

Managers must:

- ensure that all requests for Internet access serve legitimate needs of the agency.

- ensure that all users of the Internet comply with published rules and policy related to this area.

3.15 E-Mail Usage

Users must:

- Comply with all policy and procedure as outlined in the SSH on the use of e-mail.
- Inappropriate use of e-mail would include but not be limited to:

    a. forwarding chain letters or mass mailings of any type;
    b. large attachments or video or sound clips;
    c. illegal, inappropriate or offensive subject matter;
    d. commercial, business or for profit activities; and
    e. fundraising, lobbying, political activity or endorsements.

Managers must:

- Inform their employees about proper e-mail usage requirements.

- Address misuse of e-mail using general administrative agency procedures.

3.16 Procurement

Users must:

- consider security requirements in all phases of the procurement cycle: planning, solicitation, source selection and award, and contract administration.

Managers must:

- ensure that no AIS procurement request is released without prior security review and concurrence.

3.17 Privileged Users

Users must:

- not use their trusted positions and access rights to exploit system controls or access data for any reason other than in the performance of their official duties.

- never allow non-privileged users access to SSA privileged operations / functions.

Managers must:

- periodically monitor all system accesses by staff members who have special system privileges.

- ensure that proper personnel screening has been conducted prior to allowing personnel access to any SSA system with special system privileges.

4. Non-Compliance

In those instances where employees do not follow the prescribed rules of behavior, there are penalties available under existing policy and regulations ranging from official written reprimands through suspension of system privileges, temporary suspension from duty, and removal from current position, all the way to termination of employment and even criminal prosecution.

These rules of behavior are founded on the principles described in the agency's published security policy and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, Office of Management and Budget regulations and Standards of Conduct for Federal Employees. As such, they bring the same responsibility for compliance as these official documents and violations of appropriate rules are tantamount to violation of those responsibilities. For the established Agency sanctions for systems misuse, refer to ISSH Criminal Violations and Fraud.

The agency will use all existing procedures and venues currently available for dealing with non-compliance issues by members of the SSA workforce.

Systems Sanctions Violations - Agency Policy and Acknowledgement Statement

Printable Version:
Agency Policy for Systems Access, Table of Penalties, and Acknowledgment Statement by Employees

(b) (6)

Policy signed no redactions needed

September 21, 2009

To: All SSA Employees,

From: Reginald F. Wells

Deputy Commissioner for Human Resources

Subject: *Clarification* of Agency Policy for Systems Access, Table of Penalties for Violations and Acknowledgement Statement by Employees--INFORMATION

This memorandum provides notice of *minor clarifications* to the Sanctions for Unauthorized Systems Access Violations and Guidance for Employees on How to Transact Social Security Business That Requires Systems Access.

In light of Social Security Administration's (SSA) efforts to encourage the use of our "Retire Online" campaign, we *clarified* our guidance to encourage employees to refer friends, family members and former coworkers to go online to: www.socialsecurity.gov/ to file a retirement claim or take other actions related to a claim. There are several references to our website throughout the document. The only other modification was to update the link to the component privacy officers.

If you have any questions regarding the revised guidance, please contact your supervisor.

ATTACHMENT

AGENCY POLICY FOR SYSTEMS ACCESS, TABLE OF PENALTIES FOR VIOLATIONS, AND ACKNOWLEDGEMENT STATEMENT BY EMPLOYEES

I. POLICY FOR SYSTEMS ACCESS.

At the Social Security Administration (SSA), the most important resource entrusted to us by the public is the information we maintain. To ensure the integrity of that information, a set of sanctions was prepared to inform employees and managers of the importance of maintaining the security of the information maintained in SSA computer systems records and to inform them of the consequences for various types of systems security violations.

This Policy is in force to preserve the public's longstanding trust in the

Agency and its programs, including the protection of the public's right to privacy. It is also to prevent fraud and abuse of public funds, deter and correct misconduct, and hold all Agency employees to a consistent standard of behavior.

Rules contained in this Policy consolidate and clarify those previously announced (Memos issued 6-22-98, 8-9-99, and 3-2-2000), and rename the categories for clarification.

This Policy does not change the access requirements for any particular computer system. Each system may have its own rules concerning appropriate access. For example, when using such systems as FPPS or MTAS, access to a co-worker's record may be authorized and necessary. Certain personnel systems may allow an employee to access his or her own record under some circumstances. This would include actions employees can take online at www.socialsecurity.gov/.

Whenever there is doubt in any situation about whether systems access is authorized, employees must first consult with their supervisor.

A. Requesting Information about Yourself

Employees are prohibited from browsing or accessing their own records. Do not request assistance from a co-worker unless you are authorized by management to do so.

If you need to obtain information from your Social Security record or conduct business with SSA that requires systems access, you must:

Contact your supervisor, manager or management designee for advice, or

- Go to: www.socialsecurity.gov/
- Call the SSA 800 number, or
- Contact your servicing field office. However, if you work in your servicing field office, first
- contact your supervisor, manager, or management designee.

B. Requesting Information for Your Children

If you need to verify your child's social security number or conduct other business that requires systems access on behalf of a minor child in your care (e.g., file a claim for benefits, obtain a replacement social security card, obtain verification of the social security number, etc.), you must follow one of the options listed in Section A above.

In all such situations, the proper forms must be completed and appropriate documentation submitted. Children over 18, even if they are still in your care, must sign their own application and grant permission for the release of information to you.

C. Assisting Family Members

Employees are prohibited from browsing or accessing the records of their family.

If you are asked by a family member to transact Social Security business, keep in mind that the Annual Personnel Reminders require you to disqualify yourself. You should generally advise them to go online at: www.socialsecurity.gov/ or refer them to their local servicing office or the national 800 number for assistance in transacting any Social Security business.

If you work in your family member's servicing office and he or she advises you of the need to conduct business there, explain the circumstances to your supervisor, manager or management designee. They will decide on how to complete the transaction.

D. Responding to Requests for Assistance from Co-workers or Former Co-workers

A co-worker is someone who works in your facility/component or someone in another SSA facility/component with whom you interact as part of your work activity. A former co-worker is someone who has worked in this capacity with you in the past. If a current co-worker requests your assistance in obtaining personal information or transacting business for him or herself, or their child, relative or friend, you must decline and instruct the co-worker to either talk with his or her supervisor, manager or management designee, go online to: www.socialsecurity.gov/., or contact the national 800 number for assistance. The requesting employee's management official is empowered to determine how to handle the request for assistance and make the decision on how to complete the transaction and/or assign it to another employee in the office.

If a former co-worker contacts you for assistance, you should advise him or her that many actions can be taken online at: www.socialsecurity.gov/ or they should contact the servicing office manager or the national 800 number for assistance.

If an interviewer discovers during the course of an interview that an individual is a co-worker's relative or friend, the interviewer should continue to provide service to the individual. Upon completion of the interview, the interviewer must notify the supervisor or manager.

E. Responding to Requests for Assistance from Friends and Acquaintances

Realizing that many of you live in the same area in which you work and are active members of the community, it is practical to expect members of the community to request your assistance in transacting SSA-related business that requires systems access. The type of relationship you have with a member of the community will fall into two broad categories - Friend or Acquaintance – and will determine how these requests for assistance should be handled.

Friend: A friend is one to whom you are attached by affection or esteem. To ensure that your personal relationship with a friend does not cause a loss of impartiality, a request for assistance received by you from a friend should be handled in the same way requests from family members are handled. You can provide general program information about our rules and regulations, but you may not coach an individual,

obtain any queries or perform any official action on that record. See the section above on Assisting Family Members.

Acquaintance: An acquaintance is any individual in the community you may know only by name or see at various community, neighborhood or local events, but whose current relationship you do not consider rises to the level of being a friend. Requests for assistance from someone you consider only an acquaintance, and not a friend, can generally be handled to completion by you.

The Agency's key interest is in ensuring that the nature of your relationship with another does not affect your impartiality. It is expected, therefore, that you will use your good judgment, common sense, and sense of ethics in making the determination that the relationship you have with a member of the community is only that of an acquaintance, and not that of a friend.

Should a question arise about a decision you made that you were assisting an acquaintance and not a friend, management will consider several factors, including the manner and place in which the requestor made contact with you. There are some specific actions, however, that may raise questions as to the nature of your relationship with a member of the public. Such actions include handling work not assigned through established workflows, taking visitors out of turn, contacts made outside of the office followed by subsequent in-office action, handling work unrelated to your official duties, or any appearance of favoritism.

Whenever there is a reasonable doubt regarding whether you are being asked to assist a friend or an acquaintance, or there may be an appearance that your relationship with the individual requesting assistance could be seen as serving a friend or providing special treatment, as described in the paragraph above, you should consult with your supervisor, manager or management designee. They are empowered to determine who should assist the individual and how to complete the transaction in these instances.

F. Responding to Requests for Assistance from Members of Management

When members of management need to transact business for themselves or their minor children or to assist a relative or personal friend, they have several options available:

Go online to: www.socialsecurity.gov/; or call the SSA 800 number or refer friends and relatives to www.socialsecurity.gov/ or the SSA 800 number; or, contact their servicing office or refer relatives and friends to their servicing office. However, if the servicing office is the manager's office, the manager must contact his/her supervisor for handling as indicated below.

Contact their supervisor. The supervisor will determine how to handle the request for assistance and/or assign it to another employee or office to complete the transaction.

Facility heads with no onsite supervisor may refer work to another

employee in the office so long as it does not involve family members and so long as they have no further involvement in the work. If the matter involves family members of the facility head, he/she must consult with his/her supervisor, who will determine how to handle the work.

As stated in Section E above, members of management, like other Agency employees, are generally allowed to assist those in the community that are acquaintances but not friends provided that the assistance is the same that is provided to any other member of the public and not something that would be construed as a favor or special treatment.

Criminal Penalties

The disciplinary penalties listed in the attached Table of Penalties are in addition to any criminal penalties prescribed by law. SSA employees have been and will continue to be prosecuted for violations of Federal or State laws regarding privacy of records and information.

If You Need Further Information

A summary of the statutes, regulations and SSA instructions regarding privacy is in POMS, GN Part 02, Chapter 33. If you have a question that is not answered in POMS, contact your component's privacy coordinator. Each component has a coordinator to take questions and to refer them, when necessary, to the SSA Privacy Officer in Central Office. A list of coordinators can be obtained at.

http://sharepoint.ba.ssa.gov/ogc/intranet/foia_coordinators.aspx

If you have any security questions concerning the use of SSA's computer systems, you may contact the Social Security Administration Chief Information Security Officer (SSACISO), at John.T.Smith@ssa.gov or your component security officer. Regional and field employees may also call the appropriate Regional Security Officer.

Reporting Abuses

You should report any suspected abuses or concerns to your manager/supervisor and/or your Regional Security Staff.

II. TABLE OF PENALTIES FOR VIOLATIONS

This Policy includes a Table of Penalties (Table), which provides for four categories of systems access violations and the minimum required administrative penalties for corresponding offenses. Examples are provided under each category. Those examples are intended to provide some common types of situations that may apply, but do not include all possible types of violations. **Although this Table provides for minimum penalties, additional misconduct or aggravating factors may result in a more severe discipline.**

Category A – Unauthorized Access without Disclosure

An employee who improperly accesses his/her own record or another record that contains sensitive or protected information or obtains

information not related to the employee's official duties, **but does not disclose the information** commits a Category A violation. Improper access occurs because of the employee's relationship with the requester or because the access is unrelated to the employee's duties.

Example: This would include an employee accessing the record of his/her minor child to verify the SSN, looking up the record of a friend to determine his/her income or "browsing" the records of a celebrity or another member of the public.

The minimum sanctions are:

First Offense	Reprimand
Second Offense	2-day suspension
Third Offense	14 day suspension
Fourth Offense	Removal

Category B – Unauthorized Access with Disclosure to Someone Entitled to Receive the Information.

An employee who improperly accesses a record with a purpose other than personal or monetary gain or malicious intent, and discloses the information to someone entitled to the information commits a Category B sanctions violation. Access is improper based on the employee's relationship to the requestor or because it is unrelated to the employee's official duties.

Example: This would include an employee verifying information or checking on the status of a claim for a friend or relative from that person's own record and providing the information to the friend or relative.

The minimum sanctions are:

First Offense	Reprimand
Second Offense	2 day suspension
Third Offense	14 day suspension
Fourth Offense	Removal

Category C – Unauthorized Access with Disclosure to Someone Not Entitled to the Information

An employee who improperly accesses a record with a purpose other than personal or monetary gain or malicious intent, and discloses the information to someone **not** entitled to the information, commits a Category C sanctions violation. Access is improper because it is

unrelated to the employee's official duties.

Example: This would include an employee accessing the record of a friend or relative and disclosing information from that record to the spouse of the friend or relative.

The minimum sanctions are:

First Offense	14-day suspension
Second Offense	Removal*

*Removal is the minimum penalty for a second offense if there has been a prior Category C violation. A subsequent Category A or B offense will result in a minimum 15-day suspension.

Category D – Unauthorized Access for Personal Gain (including, but not limited to monetary gain) or with Malicious Intent

An employee commits a Category D sanctions violation if he or she accesses, obtains, modifies or destroys records (1) for the purpose of selling, disclosing or using the information for personal gain to himself or another; or (2) with the intent of harming another or using the records in such a manner that harming another is a reasonably foreseeable consequence; or (3) for the purpose of defrauding any SSA program or any other institution or individual; or (4) for any other purpose that results in material harm to another.

This category covers demonstrated or potential harm to the Government or a member of the public even if the employee involved did not personally profit from the incident.

Examples: This would include situations where an employee sells information from any SSA file or uses information from an SSA file to further a personal business or to harass or harm another individual. It would also include situations where the employee looks up an ex-spouse to obtain information to use against that person in a court proceeding. This category also includes situations where the employee uses information from an SSA file on behalf of any other individual. The minimum sanction for this category is:

First Offense	Removal

Resources:

The Privacy Act of 1974, the Computer Fraud and Abuse Act of 1986, the Computer Security Act of 1987, the Office of Management and Budget (OMB) Circulars A-123, A-127 and A-130, Appendix III, plus many other laws, guidelines and memorandums provide a body of regulations requiring the proper security of all Automated Information System (AIS) resources, including data.

The Privacy Act of 1974 provides guidance in the protection of personal

information maintained in Government records. The act describes what degree of protection is to be provided and prescribes sanctions and penalties for violations.

The Computer Fraud and Abuse Act of 1986 defines the willful attempt to gain unauthorized access to or misuse of information stored in Government controlled computer resources and lists appropriate penalties for violations.

The Taxpayer Browsing Protection Act of 1997 provides a criminal misdemeanor penalty for the willful, unauthorized access or inspection of Federal tax return information. The Act also required that any Federal employee who is convicted under the Act be discharged from employment.

OMB Circular A-123 requires agencies to provide and maintain internal controls on all Government programs and administrative activities.

OMB Circular A-127 prescribes policies and procedures to be followed in developing, operating and maintaining Government financial systems.

OMB Circular A-130, Appendix III, describes a minimum set of controls to be applied to all Federal AIS.

POMS, Part 02, Chapter 33 (GN 03300.000) provides a summary of the statutes, regulations and SSA instructions regarding the disclosure and privacy of SSA records.

III. ACKNOWLEDGEMENT STATEMENT

All employees are expected to read the Systems Access Policy and the Table of Penalties for Violations and be familiar with its contents. You will be asked by your supervisor to sign an Acknowledgement Statement (below), indicating that you have read and understood the Policy, whether or not you currently have authority to access any of the these systems.

1. Name _____

2. Position _____

I acknowledge I have read and understand the "Agency Policy for Systems Access, Table of Penalties for Violations". I understand that the sanctions identified in this document will be imposed for violations, including those sanctions stated for the first offense.

_____ _____

Employee's Signature Date

Home
Contact Us
Contact Site Admin

Our Organization
Mission
Org Chart

Help & Support
LRER System and Website Support
SSA Call Center #877-697-4889

Resources & Tools
CyberFeds
Federal Labor Relations Authority (FLRA)
Labor Relations Statute