

**Social Security Administration (SSA)  
System Security Requirements  
For  
Contractors & Non-Federal Organizations  
(C/NFOs)**

---



**Prepared by**

**SSA OFFICE OF INFORMATION SECURITY (OIS)**

SSA Publication No. 02-010

January 2017



## ORIENTATION

**This guide will help the reader understand and navigate through the Social Security Administration (SSA) Security System Requirements as they apply to Contractors and Non-Federal Organizations (*Contractors*).**

---

The document's purpose is to provide guidance for the protection of nonfederal systems and information, by drawing upon SSA's security controls, requirements and standards that apply to SSA vendors and other non-federal organizations, and by specifying the individual SSA security requirements that SSA contractors must comply with.

To better understand Information Protection, this document identifies what the contractor is required to accomplish. A Contractor shall:

- Ensure all SSA information is protected at rest, in transit, and in exchanges (i.e., internal and external communications).
- Limit access to SSA information to authorized personnel (those favorably adjudicated and trained) with a need-to-know, and ensure internal and external exchanges are conducted only through secure or encrypted channels. The contractor shall
- Employ encryption and approved information security standards to ensure the confidentiality, integrity, and availability of SSA information, consistent with the security controls under this publication and any security requirements specified elsewhere in the contract.

This guide is intended to help the contractor comply with the requirements, by defining the definitions, key roles and responsibilities, security categorizations and controls, as well as providing detailed guidance on how to appropriately address security for a number of different system implementation scenarios.

So, let's get started.

# TABLE OF CONTENTS

1.0	INTRODUCTION .....	1
2.0	SCOPE OF THE DOCUMENT.....	1
3.0	DEFINITIONS.....	2
4.0	DISCLOSURE OF INFORMATION.....	3
5.0	CONTRACTOR/NON-FEDERAL ORGANIZATIONS RESPONSIBILITIES .....	5
5.1	GENERAL .....	5
5.2	POLICIES AND PROCEDURES.....	5
5.3	TRAINING.....	5
5.4	INFORMATION PROTECTION .....	5
5.5	RULES OF BEHAVIOR .....	6
5.6	CONTINUOUS MONITORING OF SECURITY CONTROLS.....	6
6.0	CONTRACTOR SECURITY REVIEWS .....	6
6.1	SCOPE OF REVIEWS .....	7
6.2	COLLABORATION ON CONTRACTOR SECURITY REVIEWS.....	8
7.0	SECURITY CONTROL ORGANIZATION AND STRUCTURE.....	10
7.1	SECURITY CONTROL FAMILIES .....	10
8.0	TERMINATION OF CONTRACT .....	14
8.1	DESTRUCTION OR RETURN OF SSA INFORMATION.....	15
9.0	SYSTEM INFORMATION.....	16
9.1	SYSTEM NAME/TITLE .....	16
9.2	RESPONSIBLE NON-FEDERAL ORGANIZATION .....	16
9.3	GENERAL DESCRIPTION/PURPOSE.....	16
9.4	SYSTEM ARCHITECTURE/ENVIRONMENT .....	17
9.5	ENCRYPTION REQUIREMENTS .....	17
9.6	SSA DATA JURISDICTION RESTRICTION .....	17
10.0	APPENDIX A – SECURITY CONTROLS .....	18
10.1	ACCESS CONTROL (AC).....	18
10.2	AWARENESS AND TRAINING (AT).....	28
10.3	AUDITS AND ACCOUNTABILITY (AU) .....	29
10.4	SECURITY ASSESSMENT AND AUTHORIZATION (CA).....	32
10.5	CONFIGURATION MANAGEMENT (CM).....	35

10.6	CONTINGENCY PLANNING (CP) .....	40
10.7	IDENTIFICATION AND AUTHENTICATION (IA) .....	41
10.8	INCIDENT RESPONSE (IR).....	45
10.9	MAINTENANCE (MA).....	50
10.10	MEDIA PROTECTION (MP) .....	53
10.11	PHYSICAL AND ENVIRONMENTAL PROTECTION (PE) .....	57
10.12	PERSONNEL SECURITY (PS) .....	62
10.13	RISK ASSESSMENT (RA) .....	64
10.14	SYSTEM AND COMMUNICATIONS PROTECTION (SC).....	67
10.15	SYSTEM AND INFORMATION INTEGRITY (SI).....	73
11.0	APPENDIX B - ACRONYMS AND ABBREVIATIONS .....	78
12.0	APPENDIX C – INDEX.....	80

### **LIST OF TABLES**

TABLE 1: SAMPLE CONTROL ASSESSMENT .....	8
TABLE 2: SAMPLE SECURITY REVIEW REPORT TABLE.....	10
TABLE 3: SECURITY CONTROL FAMILIES .....	10
TABLE 4: CONTRACT TERMINATION AREAS OF REVIEW .....	14
TABLE 5: INFORMATION DESTRUCTION METHODS .....	15
TABLE 6: SYSTEM NAME/IDENTIFIER.....	16
TABLE 7: RESPONSIBLE ORGANIZATION .....	16
TABLE 8: POINT(S) OF CONTACT.....	16

# PROTECTION OF FEDERAL INFORMATION ON NONFEDERAL SYSTEMS

## 1.0 INTRODUCTION

For the reader it is important to start with the understanding that *the protection of sensitive federal information* residing in nonfederal systems and environments of operation is of paramount importance to federal agencies as it is carried out by a “Contractor” of an executive agency accessing such information, as it can directly impact the ability of the federal government to successfully carry out its designated missions and business operations.

For this reason, this publication was created as a guide to contract personnel working with information that resides in nonfederal systems and organizations, to fully understand and be compliant with the guidelines in the execution of their duties.

The following sections in this document are to be completed and returned to the SSA:

Section 11 – System Information

Section 12 – Security Controls

## 2.0 SCOPE OF THE DOCUMENT

The requirements and the security controls contained within this publication are based on the following:

- The Federal Information Security Modernization Act (FISMA) of 2014
- Office of Management and Budget (OMB) Circular A-130
- Federal Information Process Standard (FIPS) 199 Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200 Minimum Security Requirements for Federal Information and Information Systems
- Executive Order 13556 – Controlled Unclassified Information
- Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, February 2013
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, December 2016
- 32 CFR Part 2002, Controlled Unclassified Information, September 2016
- [Agency Specific Clause 2352.204-2, Federal Information Security Management Act and Agency Privacy Management](#)

- [Agency Specific \(AS\) Clause 2352.204-1, Security and Suitability Requirements \(JULY 2013\)](#)
- [SSA Information Security Policy](#)

This document addresses the security controls that need to be assessed for systems maintained by contractors and non-federal organizations not located at SSA facilities. It is for systems that store or process SSA information or that host systems on behalf of the SSA. The scope of the document does not apply to Cloud-based systems, which must comply with security requirements of the Federal Risk and Authorization Management Program (FedRAMP) in addition to the SSA specific security requirements for Cloud-based systems.

### 3.0 DEFINITIONS

**Contractors and Non-Federal Organizations (C/NFOs)** - An entity that owns, operates, or maintains a nonfederal system with whom SSA has entered into an agreement/contract with and with whom SSA must share information.

**Information** – Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms. (OMB Circular A-130)

**CUI = Controlled Unclassified Information (CUI)** - Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. [Executive Order 13556 "Controlled Unclassified Information"](#) (the Order), establishes a program for managing CUI across the Executive branch and designates the National Archives and Records Administration (NARA) as Executive Agent to implement the Order and oversee agency actions to ensure compliance.

Controlled Unclassified Information (CUI) refers to unclassified information that is to be protected from public disclosure. The SSA manages several types of CUI, such as Personally Identifiable Information (PII), Federal Tax Information (FTI), Protected Health Information (PHI), and other federal information (e.g. Building Plans, InfoSec, Critical Infrastructure, etc.).

The CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations. The protection of CUI while residing in nonfederal systems and organizations is of paramount importance to SSA and can directly impact the ability of SSA to successfully carry out its designated missions and business operations.

**PII = Personally Identifiable Information<sup>1</sup>** - Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's

---

<sup>1</sup> SSA security requirements: Contractors bidding on SSA contracts must have adequate programs in place to protect the PII information received, and protect the PII information from unauthorized use, access, and disclosure. The contractor's programs for protecting PII information received must include practices that:

- Identify all PII residing in environment
- Minimize the use, collection, and retention of PII
- Categorize PII

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. Examples of PII include, but are not limited to:

1. Name, such as full name, maiden name, mother's maiden name, or alias
2. Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
3. Address information, such as street address or email address
4. Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
5. Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

**System** - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Circular A-130)

**Federal System** - A system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

**Nonfederal System** – A system that does not meet the criteria for a federal system.

**Confidentiality** - The preserving of authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

**Integrity** - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

**Availability** - Ensuring timely and reliable access to and use of information.

## 4.0 DISCLOSURE OF INFORMATION

**Disclosure of SSA information is prohibited unless authorized by SSA.** Contractors shall have adequate programs in place to protect the information received from unauthorized use, access, and disclosure. Contractors must notify employees, contractors and subcontractors (at any tier) in detail, of the importance of protecting SSA information and the criminal or civil sanctions, penalties, or punishments that may be imposed for unauthorized disclosure or inspection. A contractor's programs for protecting information they receive must include documenting such notification to their employees, contractors and subcontractors.

- 
- Have appropriate safeguards for PII
  - Develop Incident Response Plan

To help develop further guidance for implementing and enforcing the CUI policy, a CUI Office has been established at the National Archives. Please refer to <http://www.archives.gov/cui/registry/category-list.html> for more information on CUI.



The disclosure practices and the safeguards used to protect the confidentiality of information entrusted to the government are subject to continual assessment, oversight and review, to remain fresh and current.

## **5.0 CONTRACTOR/NON-FEDERAL ORGANIZATIONS RESPONSIBILITIES**

The following sections define the SSA roles and responsibilities of the contractor security review process. SSA, at its sole discretion, reserves the right to modify the security control and enhancement requirements.

### **5.1 GENERAL**

In order to ensure SSA information and systems are protected at all times, it is the responsibility of SSA contractors to develop and implement effective information security controls and methodologies.

These controls and methodologies must be imbedded in Contractor business processes, physical environments and human capital/ personnel practices to make sure that they meet and adhere to the security controls, requirements and objectives described in this publication, and within individual contracts.

### **5.2 POLICIES AND PROCEDURES**

Contractors are responsible for developing policies and putting in place procedures to implement security controls and requirements described in this publication and the contract.

### **5.3 TRAINING**

Ensure all contractor employees who require access to SSA information or systems, regardless of their physical location, complete Security Awareness Training annually. This includes, but is not necessarily limited to, contractors or contractor personnel involved in any of the following activities:

- Manage, program or maintain SSA information in a production environment.
- Manage or operate a system or IT asset.
- Conduct testing or development of information or systems.
- Provide system administrative support.

The contractor shall maintain and furnish, as requested, records of initial and annual training and certifications. The contractor is required to establish additional internal role-based training, as needed (or as required under the terms of the contract), for personnel in the organization who require access to SSA information or systems to perform under the contract.

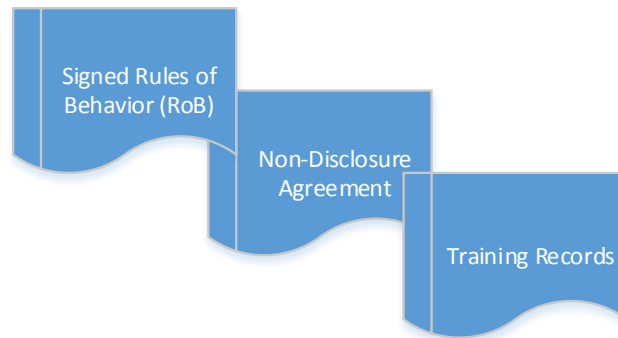
### **5.4 INFORMATION PROTECTION**

According to the requirements contained herein the contractor shall:

- Ensure all SSA information is protected at rest, in transit, and in exchanges (i.e., internal and external communications).

- Limit access to SSA information to authorized personnel (those favorably adjudicated and trained) with a need-to-know, and ensure internal and external exchanges are conducted only through secure or encrypted channels.
- Employ encryption in compliance with FIPS 140-2 to ensure the confidentiality and integrity of SSA information, consistent with the security controls under this publication and any security requirements specified elsewhere in the contract.

## 5.5 RULES OF BEHAVIOR



Contractors shall develop and distribute a set of internal rules of behavior with regard to access to and use of Government information and systems.

The Rules of Behavior, which are required in OMB Circular A-130, Appendix III, shall clearly delineate responsibilities and expected behavior of all individuals with access to systems and/or Government information.

The Contractor set of rules shall be made available to every user prior to receiving authorization for access to the system.

## 5.6 CONTINUOUS MONITORING OF SECURITY CONTROLS

Contractors must maintain ongoing awareness of their system and related security control processes to ensure compliance with security controls and adequate security of information, and to support organizational risk management decisions.

Consistent with the Continuous Monitoring process, whenever security controls are identified as out of compliance, contractors must track, manage, and remediate the controls. If the deficient security controls result in an incident or if an incident is imminent, or if there is a serious weakness with potential to impact SSA it must be reported to SSA using the incident reporting procedures. For additional guidance, see Section 12.8, IR-6 Incident Reporting.

## 6.0 CONTRACTOR SECURITY REVIEWS

Contractor security reviews are subject to the Terms and Conditions of the contract.

Security controls are defined as the management, operational, and technical safeguards or countermeasures employed to protect the confidentiality, integrity and availability of an organization's information and systems.

The contractor must provide the Contracting Officer Representative (COR) current documentation that indicates in-place and planned security changes. The completion of Section 11 and Appendix A fulfills this documentation requirement for contractors and non-federal organizations that process SSA information.

## 6.1 SCOPE OF REVIEWS

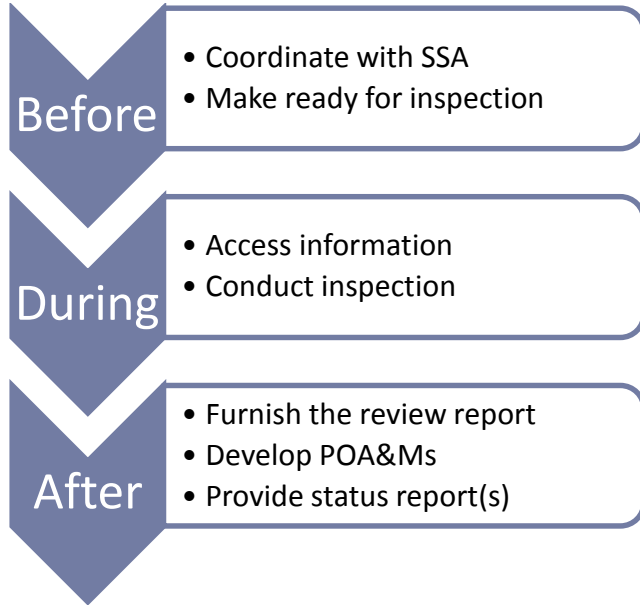
Contractor Security Reviews typically concentrate on the following key areas:

- **System or information**, itself;
- **Physical environment** in which the system or information is handled or processed; and
- **Personnel** who have access to or are responsible for handling or processing the system or information.

The security review will typically include the following:

- **Risk Management.** Identification of weaknesses, threats, and vulnerabilities, and recommendations for remediation.
- **Control Evaluation.** Evaluation of all applicable SSA security controls.
- **Background Checks.** Verification of all personnel security background checks for all contractor employees working on SSA contract, including subcontractor employees, and IT support personnel (at any tier) that have access to SSA information or systems.
- **System Configurations.** Validation of IT security configurations including workstations, servers, routers, and switches.
- **Training Verification.** Verification of employees' completion of SSA mandated Security Awareness Training (SAT). The Security Awareness Training is composed of modules of Information Protection briefings on: system security, disclosure, privacy, physical security, and/or unauthorized access commensurate with the assigned risk designations of the position for the work being performed and the category of SSA information to which the employee has access. The SAT training is to be completed annually and completion documented per contractor.
- **Scans.** Performance of vulnerability scans.

## 6.2 COLLABORATION ON CONTRACTOR SECURITY REVIEWS



Before the review: Contractors shall coordinate with SSA on all aspects of preparation of the review including, but not limited to, agreement on time(s) and place(s) of review, and timely submission of any pre-site visit materials, as requested, and making ready for inspection, all other policies, documentation, and records that shall be needed at the time or during the review.

During the review: The contractor shall make its facilities, installations, operations, documentation, records, databases and personnel available to SSA to carry out a program of inspection (in a manner not to unduly delay the work) to safeguard against threats and hazards to the security, confidentiality, integrity, and availability of Government data.

Access to contractor facilities and SSA information or systems by SSA inspectors/reviewers shall be permitted, in accordance with the terms of the contract, subject to confirmation of identity, which shall be based on each person presenting an active (unexpired), Government issued Personal Identity Verification (PIV) card.

**Table 1: Sample Control Assessment**

Control # and Name	#	Control Description	Control Implementation
<b>Security (SE)</b>			
<b>SE-2 Privacy Incident Response</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place )	01	The organization: a. Develops and implements a Privacy Incident Response Plan; and	Includes the control status, observations, weaknesses, and recommendations.

Control # and Name	#	Control Description	Control Implementation
<input type="checkbox"/> Planned (Not in Place)			
	02	The organization: b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.	Includes the control status, observations, weaknesses, and recommendations.

After the review: Within 45 days of the completion of the Contractor Security review, the assessor shall furnish the completed System Security Requirements Report.

The report contains:

- Identifier:** All weaknesses are assigned a vulnerability ID in the form of V#-Security Control ID. For example, the first vulnerability listed would be reported as V1-AC-2(2) if the vulnerability is for control ID AC-2(2). If there are multiple vulnerabilities for the same security control ID, the first part of the vulnerability ID must be incremented, for example V1-AC-2(2), V2-AC-2(2).
- Name:** A short name unique for each vulnerability.
- Source of Discovery:** The source of discovery refers to the method that was used to discover the vulnerability (e.g. web application scanner, manual testing, security test procedure workbook, interview, document review). References must be made to scan reports, security test case procedures numbers, staff that were interviewed, manual test results, and document names. If the source of discovery is from an interview, the date of the interview and the people who were present at the interview are named. If the source of discovery is from a document, the document must be named.
- Description:** All security weaknesses must be described well enough such that they could be reproduced by the CSP, the ISSO, or the AO. If a test was performed manually, the exact manual procedure and any relevant screenshots must be detailed. If a test was performed using a tool or scanner, a description of the reported scan results for that vulnerability must be included along with the vulnerability identifier (e.g. CVE, CVSS, and Nessus Plugin ID etc.) and screenshots of the particular vulnerability being described. If the tool or scanner reports a severity level, that level must be reported in this section. Any relevant login information and role information must be included for vulnerabilities discovered with scanners or automated tools. If any security weaknesses affect a database transaction, a discussion of atomicity violations must be included.
- Affected IP Address/Hostname(s)/Database:** For each reported vulnerability, all affected IP addresses/hostnames/databases must be included. If multiple hosts/databases have the same vulnerability, list all affected hosts/databases.

- **Recommendation:** The recommendation describes how the vulnerability must be resolved. Indicate if there are multiple ways that the vulnerability could be resolved or recommendation for acceptance of operational requirement.

**Table 2: Sample Security Review Report Table**

Identifier	Name	Source of Discovery	Description	Affected IP Address / Hostname / Database	Recommendation

## 7.0 SECURITY CONTROL ORGANIZATION AND STRUCTURE

This document provides the reader with information on required security controls for protecting SSA information. These security controls are organized into families where each security control family contains security controls related to the functionality of the family. A two-character identifier is assigned to uniquely identify each security control family.

The following tables summarize the family of controls and associated identifiers for developing security controls used in this publication, listed alphabetically.

### 7.1 SECURITY CONTROL FAMILIES

There are fifteen (15) security control families that non-federal organizations must consider when processing SSA information

**Table 3: Security Control Families**

Code	Control Designation
AC	<a href="#">Access Controls</a>
AT	<a href="#">Awareness &amp; Training</a>
AU	<a href="#">Audit and Accountability</a>
CA	<a href="#">Security Assessment and Authorization</a>
CM	<a href="#">Configuration Management</a>
CP	<a href="#">Contingency Planning</a>
IA	<a href="#">Identification and Authentication</a>
IR	<a href="#">Incident Response</a>
MA	<a href="#">Maintenance</a>
MP	<a href="#">Media Protection</a>
PE	<a href="#">Physical and Environmental Protection</a>
PS	<a href="#">Personnel Security</a>
RA	<a href="#">Risk Assessment</a>
SC	<a href="#">System and Communications Protection</a>

Code	Control Designation
SI	<a href="#">System and Information Integrity</a>

### **Access Control (AC)**

Access controls provided security controls required to restrict access to information and to systems. Information shall be restricted to those contractors who have a valid background check and a need to know.

### **Awareness and Training (AT)**

SSA has established policies and procedures to ensure awareness training and role-based training take place at contractor sites.

### **Audits and Accountability (AU)**

The contractor shall enable auditing on those assets to ensure that actions shall be logged, and so that access to SSA information shall be monitored and tracked.

### **Security Assessment and Authorization (CA)**

An assessment of security controls provides the contractor and SSA with an assurance that security controls are established and operating, as intended, within the contractor environment. Key points of this process include:

- Conducting an independent information security assessment to ensure the contractor-defined security controls are operating as intended,
- Identification of weaknesses/vulnerabilities,
- Briefing management of weaknesses/vulnerabilities,
- Formal SSA acceptance of any associated risks or mitigation of risks or implementation of compensating controls, and
- Accrediting the environment by authorizing the environment to be operational, by a senior contractor official.

Assurances shall be made to ensure security controls have been applied; that testing has been conducted to validate controls; and that a designated official has authorized the use of the IT assets, and identified any risks accepted by the contractor management.

### **Configuration Management (CM)**

Configuration management ensures that organizations are using the correct versions of procedures and processes and that there are formal mechanisms in place to implement new procedures and processes.

### **Contingency Planning (CP)**

All contractors shall develop a contingency plan and business resumption plan to provide information for how the contractor shall restore business operations and resume business in the event of failed IT assets or the inability to access the facility.

### **Identification and Authentication (IA)**



Identification and authentication is a process that is used to identify an individual (e.g. user name) to the system and authenticate (e.g. password, token, multifactor solutions) the individual, prior to allowing access to a system, such as a workstation, laptop, server, etc.

### **Incident Response (IR)**

Whenever there is a compromise of SSA information, contractors shall contact SSA within one hour of detection. SSA shall work closely with SSA contractors to quickly respond to a suspected incident of unauthorized disclosure or inspection.

An incident is a violation or suspected violation of information security policies and practices as required by this document, and implemented by your business. Types of incidents include the following:

- **Denial of Service** - An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
- **Malicious Code** – A virus, worm, Trojan horse, or other code-based malicious entity that infects a host.
- **Unauthorized Access** – A person or system, without permission, gains logical access or physical access to a network, system, application, data, or other resource.
- **Inappropriate Usage** – A person violates acceptable system use policies or improperly uses SSA data.
- **Multiple Components** – A single incident that encompasses two or more characteristics of other incident types.
- **Theft** – Removal of system, data/records, on system media or paper files.
- **Loss/Accident** – Accidental misplacement or loss of systems, data/records on system media or paper files
- **Disclosure of Sensitive Data** –The unauthorized, inadvertent, or deliberate disclosure of SSA data.

### **Maintenance (MA)**

Maintenance ensures that all IT assets are able to be used and ensures the integrity and reliability of the equipment. All contractors, small and large, shall rely on the operation and functionality of equipment if they are to provide continued service to SSA.

### **Media Protection (MP)**

Media protection controls ensure that all removable media are adequately secured to allow for the deterrence, detection, reporting, and management of loss, theft, or destruction. An inventory should be maintained and provided to SSA, upon request that identifies all media used to store, maintain, or process SSA information

Any media that are used to store, maintain, or process SSA information cannot be commingled with non-SSA data. All SSA information being handled or processed by the contractor must be segregated from other work being performed either logically and/or physically.

### **Physical and Environmental Protection (PE)**

Physical security shall be provided for a document, an item, or an area in a number of ways. The physical security controls include, but are not limited to, locked containers of various types, vaults, locked rooms, locked rooms that have reinforced perimeters, locked buildings, guards, electronic

security systems, fences, identification systems, and control measures. How the required security is provided depends on the facility, the function of the activity, how the activity is organized, and what equipment is available.

Proper planning and organization shall enhance the security while balancing the costs.

The controls are intended to protect moderate information and systems at SSA. It is not the intent of SSA to mandate requirements to those systems and/or areas that are not handling and processing SSA information.

The Minimum Protection Standards (MPS) establish a uniform method of protecting information and items that require protecting. These standards contain minimum standards that shall be applied on a case-by-case basis. Since local factors shall require additional security measures, management shall analyze local circumstances to determine space, container, and other security needs at individual facilities. The MPS have been designed to provide management with a basic framework of minimum security requirements.

Care shall be taken to deny unauthorized access to areas containing SSA information during duty and non-duty hours. This can be accomplished by creating restricted areas, security rooms, or locked rooms. Additionally, SSA information in any form (system printout, photocopies, tapes, notes, etc.) shall be protected during non-duty hours. This can be done through a combination of methods: secured or locked perimeter, secured area, or containerization.

The objective of MPS standards is to prevent unauthorized access to SSA information.

MPS requires two barriers to access SSA information under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Locked means that an area or container has a lock, and that the keys or combinations are controlled. A security container is a lockable metal container with a resistance to forced penetration, with a security lock and keys or combinations are controlled. The two barriers provide an additional layer of protection to deter, delay, or detect surreptitious entry. Protected information shall be containerized in areas where other than authorized employees shall have access after-hours.

Using a common situation as an example, often an organization desires or requires that security personnel or custodial service workers have access to locked buildings and rooms. This shall be permitted as long as there is a second barrier to prevent access to SSA information. A security guard shall have access to a locked building or a locked room if SSA information is in a locked container. If SSA information is in a locked room, but not in a locked container, the guard or janitor shall have a key to the building but not the room.

### **Personnel Security (PS)**

All contractor and subcontractor employees performing or proposed to perform under the contract are identified to SSA at time of award (or assignment) in order to initiate appropriate background investigations. Any personnel that are not favorably adjudicated or otherwise pose a security risk are immediately removed from performance under contracts with SSA, and suitable replacement personnel agreeable to SSA are provided.

### **Risk Assessment (RA)**

Risk assessment controls ensure that risk can be assessed within the organization, and that appropriate mitigation controls can be implemented.

## System and Communications Protection (SC)

A secure system communication ensures that information is protected from unauthorized disclosure or tampering during transit, and ensures that the network communication paths, where IT assets are being used to transmit SSA information, are protected.

## System and Information Integrity (SI)

This section applies to contractors, who are developing application programs, web-based interface applications, surveys that can be completed by a user population, and other instances where input data could be manipulated, causing inaccurate information to be generated. For each control, there shall be a note on the applicability to a contractor site.

## 8.0 TERMINATION OF CONTRACT

In addition to maintaining security requirements for the duration of the contract, a Contractor is also obliged to secure information and systems at the end of the contract period. The following are guidelines for information safety at the end of a contract:

At the end of the contract period, or if the contract is terminated within the contract period, the contractor shall coordinate with SSA to ensure contractor and contractor employee access privileges to SSA information, SSA systems and facilities are revoked in a timely manner.

Contractors shall confirm to SSA officials that information furnished under the contract has been returned, disposed, or properly destroyed. Information and IT assets shall be returned to SSA, destroyed and/or sanitized, as required or directed by SSA. This includes assuring SSA that all IT assets, including laptops, systems, servers, routers, printers, faxes, switches, voice recordings, and all removable and fixed media have been sanitized of all SSA information prior to returning into production for other use.

Contractors required to return SSA information and property (as a part of the contract requirements) shall use a process that ensures that the confidentiality of SSA information is protected at all times during transport.

A log shall be maintained that identifies for all media destroyed, the date of destruction, content of media, serial number, type of media (e.g., CD, DVD, Closed Circuit Television (CCTV), etc.), destruction performed, personnel performing destruction, and witness(es). If any SSA information was stored on these devices, then VoIP devices shall be sanitized prior to returning to production. All hard drives and removable media shall be inventoried, sanitized, and logged to demonstrate data destruction for all IT assets used to handle SSA data. All hard copies shall be returned to SSA.

**Table 4: Contract Termination Areas of Review**

Area of Review	Areas of Concern
Account access privileges	SSA information, systems, and facilities
Information disposition (return, disposal, destruction, sanitization)	IT assets: laptops, systems, servers, routers, printers, faxes, switches, voice recordings, removable and fixed media

Area of Review	Areas of Concern
Property return	SSA information and property
Tracking log (date of destruction, content of media, serial number, type of media, destruction performed, personnel performing destruction, and witness(es))	Hard drives, removable media, and hardcopies

## 8.1 DESTRUCTION OR RETURN OF SSA INFORMATION

When the contract is officially closed out, SSA information provided to the contractor or created by the contractor shall be returned to SSA or destroyed as directed in writing by SSA. This includes copies of reports, extra copies, photo impressions, system printouts, carbon paper, notes, stenographic notes, and work papers.

Destruction of media is the ultimate form of sanitization. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, crosscut shredding, incineration, pulverizing, and melting. The shred size of the refuse shall be small enough that there is reasonable assurance that the information cannot be reconstructed.

**Table 5: Information Destruction Methods**

Type	Paper	Media (Fixed and movable)
Examples	Copies of reports, extra copies, photo impressions, system printouts, carbon paper, notes, stenographic notes, work papers	Laptops; systems; servers; routers; printers; faxes; switches; magnetic, video, and voice recordings; removable (e.g., optical media: CDs, DVDs); and fixed media (e.g., hard drives)
Disintegration	n/a	Yes
Shredding	Yes	Yes
Degauss	n/a	Yes
Incineration	Yes	Yes
Pulverizing	n/a	Yes
Melting	n/a	Yes

An SSA employee shall be present during the incineration and/or destruction of SSA information. If an SSA employee is not present, cleared contractor personnel shall be present.

## 9.0 SYSTEM INFORMATION

### 9.1 SYSTEM NAME/TITLE

Table 6: System Name/Identifier

System Name/Title:	System ID No:
<SSA system name> (short name-subsystem short name)	

### 9.2 RESPONSIBLE NON-FEDERAL ORGANIZATION

Table 7: Responsible Organization

Organization Name	Address

Table 8: Point(s) of Contact

<b>Name:</b>	
<b>Title:</b>	
<b>Organization:</b>	
<b>Address:</b>	
<b>Telephone:</b>	
<b>Email:</b>	
<b>Responsibility:</b>	[Organization Name] [Role]

### 9.3 GENERAL DESCRIPTION/PURPOSE

[This section should contain a detailed general description and overall purpose for the system. It should identify the system's purpose, capabilities, users, arrangements for hosting, connection and/or interface to SSA, and information data flow; discuss the hardware, software and firmware implemented in support of the system] ← DELETE

## 9.4 SYSTEM ARCHITECTURE/ENVIRONMENT

[Provide a description of the system architecture/environment, explaining where and by whom it is hosted, whether it is a web-based (or cloud, etc.) application, what Software (SW) it is utilizing, what SW sits on the front end, back end, OS, how many users access the system, describe user interfaces, and designate whether connectivity to SSA and/or the outside is through VPN or WAN, etc.] ← DELETE

[INSERT a diagram of the system architecture, including it's interconnections/interfaces/other relationships to SSA and any other third parties]. ← DELETE

## 9.5 ENCRYPTION REQUIREMENTS

In order to ensure security of SSA's information, the contractor shall adhere to the following requirements:

- SSA data on mobile computers/devices and removable media must be encrypted.
- All SSA sensitive data transmitted in either direction beyond the SSA Network, (i.e., external to the firewall) *must* be encrypted or otherwise protected as approved by 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. The key must be delivered in a manner that the key is not physically attached to the media, or shipped in the same package.
- Encryption-related information (such as keys) must be secured when unattended or not in use.
- Only FIPS-140-2 compliant encryption software must be used.
- The encryption method employed must meet acceptable standards designated by the National Institute of Standards and Technology (NIST). The encryption method to secure data for use by SSA is the Advanced Encryption Standard (AES) with a minimum 128-bit cipher.

### Laptops

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

## 9.6 SSA DATA JURISDICTION RESTRICTION

The contractor must ensure that SSA data is stored and processed within U.S. government jurisdictions, possessions, and territories.

## 10.0 APPENDIX A – SECURITY CONTROLS

Organizations employ security controls in federal systems and the environments in which those systems operate. The minimum security control baseline for this system is documented below. Specifically, this section provides a description of how all the minimum security controls are being implemented or how they will be implemented in the future.

Completion of Appendix A requires that the applicable Implementation Status box(es) of each security control be checked (i.e., left column) and the supporting information be entered in the ‘Control Implementation’ column for each control.

### 10.1 ACCESS CONTROL (AC)

Control# and Name	#	Control Description	Control Implementation
Access Control (AC)		Access controls restrict access to information and systems. Information shall be restricted to those contractors who have a valid background check and a need to know.	
<b>AC-2 Account Management</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	Each user and administrator shall have a unique account when using an IT asset, such as a server, network, or system when performing SSA work.	

Control# and Name	#	Control Description	Control Implementation
	02	There shall be a procedure that briefly describes how these accounts shall be established, reviewed at least annually, modified, or removed, as necessary.	
	03	At a minimum, the contractor shall identify all personnel authorized to access the IT asset, including system support personnel.	
	04	<u>Control Enhancements:</u> (1) Automated System Account Management The contractor employs automated mechanisms to support the management of system accounts.	
	05	(2) Removal of Temporary/Emergency Accounts The system automatically disables temporary and emergency accounts after 48 hours.	
	06	(3) Disable Inactive Accounts The system automatically disables inactive accounts after 90 days and the account must be removed within 1 year.	
	07	(4) Automated Audit Actions The system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	



Control# and Name	#	Control Description	Control Implementation
<b>AC-3 Access Enforcement</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall develop a management process that demonstrates how contract employees are approved for access, prior to being authorized access to IT assets used for SSA work.	
<b>AC-4 Information Flow Enforcement</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	Systems containing SSA information may not be interconnected to any other systems without written approval from SSA. Additionally, the data may not be transmitted externally in clear text.	
<b>AC-5 Separation of Duties</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall establish appropriate divisions of responsibilities and separations of duties as needed to prevent malicious activity without collusion.	

Control# and Name	#	Control Description	Control Implementation
	02	Whenever there are multiple contractors performing information technology support, the contractor shall develop and maintain a roster showing the roles and responsibilities for maintaining the information and the system, ensuring there are checks and balances in place for all IT processes.	
<b>AC-6 Least Privilege</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall ensure that users access is limited to only those functions required to perform their specific duties.	
	02	Employees performing data entry would not require System Administrator or elevated privileges.	
	03	Electronic, optical, and other digitally maintained media shall be restricted to prevent unauthorized access. Access is to be restricted to ‘need to know’ and ‘least privilege.’	
	04	<u>Control Enhancements:</u> (1) Authorize Access to Security Functions  The contractor explicitly defines the list of security functions and authorizes access to those functions using privileged accounts only.	

Control# and Name	#	Control Description	Control Implementation
	05	<p>(5) Privileged Accounts</p> <p>The contractor restricts privileged accounts on the system to individuals assigned to roles that require such access, such as system administrators and network technicians.</p>	
	06	<p>(2) Non-Privileged Access For Nonsecurity Functions</p> <p>The contractor requires that users of system accounts, or roles, with access to security functions including but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.</p>	
	07	<p>The system prevents non-privileged users from executing privileged functions.</p>	
<p><b>AC-7 Unsuccessful Login Attempts</b></p> <p><b>Implementation Status:</b> (check all that apply):</p> <p><input type="checkbox"/> Implemented (In Place )</p> <p><input type="checkbox"/> Planned (Not in Place)</p>	01	<p>All IT assets must be configured to enforce a limit of three (3) consecutive invalid logon attempts by a user within a 15-minute period.</p>	

Control# and Name	#	Control Description	Control Implementation
	02	Upon a third unsuccessful logon attempt, the user's account shall be automatically locked. The account is to remain locked until unlocked by an system administrator or authorized person or password reset function).	
	03	All visible information shall be removed from screen view.	
<b>AC-8 System Use Notification</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	For any systems/applications being used, the system or application shall display an SSA approved system usage notification (e.g., warning banner) before granting system access.	
	02	The warning banner shall state:  “(i) only authorized users can access this system. This system is a U.S. Government computer system subject to federal law; (ii) system usage shall be monitored, recorded and subject to audit; (iii) unauthorized use of the system is prohibited and subject to disciplinary, civil action or criminal prosecution, and (iv) that the use of the system indicates consent to monitoring and recording.”	

Control# and Name	#	Control Description	Control Implementation
<b>AC-11 Session Lock</b> <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	When a contractor uses an IT asset for SSA work, the IT asset shall be locked whenever the asset is left unattended.	
	02	When a session lock is established, the system, or application shall remain locked until the user provides appropriate identification and authentication.	
<b>AC-12 Session Termination</b> <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The system terminates a user session after 15 minutes of inactivity.	
	02	All visible information shall be removed from screen view.	
<b>AC-17 Remote Access</b> <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall disable remote access to assets supporting SSA work. Remote access must be explicitly authorized by SSA.	

Control# and Name	#	Control Description	Control Implementation
	02	Authorized remote access must be secured using a certificate-based encryption solution, such as, a Virtual Private Network (VPN) solution.	
	03	The use of 2-factor authentication where one of the authentication factors is a physical token, such as a Personal Identity Verification (PIV) card, is required.	
	04	<u>Control Enhancements:</u> (1) Automated Monitoring / Control The contractor employs automated mechanisms to facilitate the monitoring and control of remote access methods.	
	05	(2) Protection of Confidentiality / Integrity Using Encryption The contractor uses cryptography to protect the confidentiality and integrity of remote access sessions. The encryption mechanism must be a validated FIPS 140-2 compliant solution.	
	06	(3) Managed Access Control Points The system routes all remote accesses through a limited number of managed access control points.	

Control# and Name	#	Control Description	Control Implementation
<b>AC-18 Wireless Access</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	Wireless access must be based on the MAC address and configured to WPA-2 and AES 256 standards. Bluetooth is not permitted.	
<b>AC-19 Access Control for Mobile Devices/ Platforms</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	All mobile computing devices (e.g., laptop, tablet, mobile devices/platforms) shall be configured with full disk encryption and be password protected.	
	02	SSA data may not be stored on removable media without explicit written consent by SSA. This includes CD, DVD, USB/Thumb drives, optical and portable hard drives.	
	03	Any data stored on removable media with permission by SSA must be encrypted to comply with FIPS 140-2.	
	04	Such media shall be kept in a secured area under the immediate protection and control of an authorized employee or locked up.	

Control# and Name	#	Control Description	Control Implementation
	05	When not in use, the media shall be promptly returned to a proper storage area/container.	
	06	No personally-owned storage devices may be used to store SSA data under any circumstances.	
	07	All laptops are required to have full disk encryption that complies with current Federal Information Processing Standards (FIPS) Publication 140-2 requirements.	
<b>AC-20 Use of External Systems</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	No SSA data shall be stored on external systems not covered under the scope of the contract or agreement with SSA without explicit written consent by SSA.	
<b>AC-22 Publicly Accessible Content</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall prevent any unauthorized modification of data provided by SSA.	



## 10.2 AWARENESS AND TRAINING (AT)

Control# and Name	#	Control Description	Control Implementation
Awareness and Training (AT)		SSA has established policies and procedures to ensure awareness training and role-based training take place at contractor sites.	
<b>AT-2 Security Awareness</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall comply with the security awareness requirements (i.e., <a href="#">OAG</a> clause) stated in the contract.	
	02	Annual Information Security Awareness Training is required for the contractor organization. Role-Based training is required for individuals with significant information security responsibilities, for those responsible for retention of training evidence. Reporting to SSA is upon request.	
	03	User training pertaining to mobile devices/platforms is required. Training should cover not leaving the device unguarded.	

### 10.3 AUDITS AND ACCOUNTABILITY (AU)

Control# and Name	#	Control Description	Control Implementation
<b>Audits and Accountability (AU)</b>		<b>The contractor shall enable auditing on those assets to ensure that actions shall be logged, and so that access to SSA information shall be deterred, monitored, and tracked.</b>	
<b>AU-2 Audit Events</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	At contractor sites, auditing shall be accomplished to record and monitor access to IT assets storing SSA data.	
	02	Audit records shall be sufficient to enable re-creation of system related events.	
	03	The contractor shall identify and enable auditable events that shall allow the contractor to detect, deter, and report on suspicious activities.	
	04	The minimum events to be audited include: a. Logon/logoff events b. Account Management c. Privilege or role changes d. Administrator activity e. Deletion, modification, or access of sensitive data.	

Control# and Name	#	Control Description	Control Implementation
	05	Access logs should be maintained to audit access attempts.	
<b>AU-3 Content of Audit Records</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	Audit records must contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.	
<b>AU-5 Response to Audit Processing Failures</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	In the event that the audit records become full and/or auditing stops recording, the system shall be configured, so that an alert is generated, and appropriate management is notified to take action to ensure audit record is retained and the system is returned to normal operations.	
<b>AU-6 Audit Review, Analysis, and Reporting</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	Automated reports shall be generated, and management or designated personnel shall review reports to identify unusual activity and take action, as necessary.	

Control# and Name	#	Control Description	Control Implementation
	02	The contractor shall \ be conducting reviews every two weeks as a minimum.	
	03	For any compromise to SSA information, this shall be identified as an information security incident, and reported to the SSA. See procedures in Incident Response and Incident Reporting section of this document.	
	04	Audit reports shall be developed, using a user readable format to enable a manager or designated official to readily identify significant events. These events shall be reviewed for unusual activities, suspicious activities or suspected violations.	
<b>AU-8 Time Stamps</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	All audit records shall use a system generated time stamp to capture the date and time of an event being captured.	
	02	For networks that cross time zones, internal system clocks shall be synchronized with an authoritative time source.	

Control# and Name	#	Control Description	Control Implementation
<b>AU-9 Protection of Audit Information</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	System audit records shall be protected from unauthorized access, modification, and deletion.	
	02	<u>Control Enhancements:</u>  (4) Access by Subset of Privileged Users  The contractor shall authorize access to management of the audit functionality to a tightly-controlled subset of privileged users.	

#### 10.4 SECURITY ASSESSMENT AND AUTHORIZATION (CA)

Control# and Name	#	Control Description	Control Implementation
Security Assessment and Authorization (CA)		<b>An assessment of security controls provides the contractor and SSA with an assurance that security controls are established and operating, as intended, within the contractor environment. Key points of this process include:</b>	

Control# and Name	#	Control Description	Control Implementation
		<ul style="list-style-type: none"> <li>• <b>Conducting an independent assessment to ensure the contractor-defined security controls are operating as intended,</b></li> <li>• <b>Identification of weaknesses/risks,</b></li> <li>• <b>Briefing management of weaknesses/risks,</b></li> <li>• <b>Formal SSA acceptance of any associated risks or mitigation of risks or implementation of compensating controls, and</b></li> <li>• <b>Accrediting the environment by authorizing the environment to be operational, by a senior contractor official.</b></li> </ul> <p><b>Assurances shall be made to ensure security controls have been applied; that testing has been conducted to validate controls; and that a designated official has authorized the use of the IT assets, and identified any risks accepted by the contractor management.</b></p>	
<b>CA-2 Security Assessments</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	An independent assessment shall be conducted to validate that the security controls have been appropriately defined and are operating as intended for all IT assets.	

Control# and Name	#	Control Description	Control Implementation
	02	This assessment shall be conducted periodically or when major changes have been made to the IT environment to ensure the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the IT environment.	
	03	This security requirements document shall be produced with the results of the assessment and that the report is to be provided to the SSA COR or designated representative.	
	04	<u>Control Enhancement:</u> (1) Independent Assessors The contractor employs an independent assessor or assessment team to conduct an assessment of the security controls in the system.	
<b>CA-5 Plan of Action and Milestones (POA&amp;M)</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	For any security reports issued to the contractor, including internal independent reviews, the contractor is responsible for developing a Plan of Action and Milestone (POA&M) that identifies corrective actions and/or mitigating controls for any identified vulnerabilities.	

Control# and Name	#	Control Description	Control Implementation
	02	Contractors shall report to COR POA&M progress at least monthly.	
	03	In addition, the contractor must provide artifacts to update POA&M items at least 7 days prior to milestone completion date to ensure SSA has sufficient time to review.	

### 10.5 CONFIGURATION MANAGEMENT (CM)

Control# and Name	#	Control Description	Control Implementation
<b>Configuration Management (CM)</b>		Configuration management ensures that organizations are using the correct versions of procedures and processes and that there are formal mechanisms in place to implement new procedures and processes.	
<b>CM-2 Baseline Configuration</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall develop, document, and maintain a current baseline configuration for all IT assets. This inventory shall include all databases, applications, etc. that are being used as part of the baseline configuration for servers, routers, workstations, etc. Operating system baselines are required for all devices, and applications need baselines as well.	
	02	All baselines shall be reviewed at least annually.	



Control# and Name	#	Control Description	Control Implementation
	03	Control Enhancements: (1) Reviews and Updates The contractor reviews and updates the baseline configuration of the system: a. Annually, b. When required due to a significant change, and c. As an integral part of system component installations and upgrades.	
	04	(3) Retention of Previous Configurations The contractor retains older versions of baseline configurations as deemed necessary to support rollback.	
	05	(7) Configure Systems, Components, or Devices For High-Risk Areas The contractor issues systems, system components, and/or devices with appropriately hardened configurations to individuals traveling to locations that the organization deems to be of significant risk; and examines and applies appropriate safeguards to the devices when the individuals return.	
<b>CM-3 Configuration Change Control</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place )	01	The contractor shall develop and implement a change control process. This process shall ensure that all changes are approved, tested and documented using a change control log.	

Control# and Name	#	Control Description	Control Implementation
<input type="checkbox"/> Planned (Not in Place)			
	02	This change control log shall be retained for SSA.	
<b>CM-4 Security Impact Analysis</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall assess all system or application changes to determine if there is any impact to the security controls that shall be created by proposed changes.	
	02	Artifacts are to be retained for SSA review.	
<b>CM-5 Access Restrictions for Change</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall ensure that permissions are applied to the systems and applications to ensure that only authorized personnel shall make changes to the systems and applications following change control processes.	
	02	All changes made to the system or application shall be documented.	

Control# and Name	#	Control Description	Control Implementation
<b>CM-6 Configuration Settings</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall establish a baseline configuration using NIST checklists that shall be applied to the IT environment. Automated tools shall be used to ensure compliance with the IT security configurations. Automated tools shall include any of those identified by NIST.	
	02	Systems shall only have essential capabilities for ports, protocols, and services.	
	03	All vendor passwords or passwords issued for systems and applications shall be changed, including default passwords.	
<b>CM-7 Least Functionality</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	Protocols, Services and Logical Ports that shall be restricted include, but are not limited to File Transfer Protocol (FTP), Telnet, Structured Query Language (SQL) services enabled on non-SQL servers, and Universal Serial Bus (USB) ports.	
	02	Control Enhancements:  (1) Periodic Review  The contractor organization reviews the system at least annually to ensure compliance.	

Control# and Name	#	Control Description	Control Implementation
	03	(5) Authorized Software / Whitelisting  The contractor organization maintains a list of authorized software programs and prohibits execution of other software on the system. The contractor organization shall provide the authorized list for SSA reviews.	
<b>CM-8 System Component Inventory</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned  (Not in Place)	01	The contractor shall develop and maintain an inventory of all hardware, software, and removable media to support SSA work. The inventory shall include inventory serial number, description of the inventory item, owner of the inventory item, date placed in inventory, and date inventory was validated.	
	02	At a minimum, the inventory shall be reviewed and reconciled annually.	
	03	Inventory shall be sufficient to enable recovery of IT assets that are identified as lost, stolen, or disclosed.	
	04	Control Enhancements:  (1) Updates During Installations / Removals  The contractor updates the inventory of system components as an integral part of component installations, removals, and system updates.	

## 10.6 CONTINGENCY PLANNING (CP)

Control# and Name	#	Control Description	Control Implementation
<b>Contingency Planning (CP)</b>		All contractors shall develop a contingency plan and business resumption plan to provide information for how the contractor shall restore business operations and resume business in the event of failed IT assets or the inability to access the facility.	
<b>CP-9 System Backup</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	For contractors with systems, in order to achieve the Recovery Point Objective (RPO) and the Recovery Time Objective (RTO) of the business customer, the contractor shall back up data contained in the systems to enable contractors to provide continuous support to SSA.	
	02	The contractor shall test backup restoration capability to ensure information could be recovered, as necessary.	
	03	A Business Continuity Plan (BCP) must be provided to SSA to include the maximum recovery time, and the maximum data loss.	
	04	The BCP should account for geographic diversity is dependent on the level of impact.	
	05	The BCP must include the method of backup and recovery, secure backup media if created, severity and handling of backup media, and testing.	
	06	Backup media is to be retained in the continental U.S.A., possessions, or its territories.	

Control# and Name	#	Control Description	Control Implementation
	07	Control Enhancements: (1) Testing For Reliability / Integrity The contractor tests backup information semi-annually to verify media reliability and information integrity.	

### 10.7 IDENTIFICATION AND AUTHENTICATION (IA)

Control# and Name	#	Control Description	Control Implementation
<b>Identification and Authentication (IA)</b>		Identification and authentication is a process that is used to identify an individual (e.g. user name) to the system and authenticate (e.g. multifactor authentication or token) the individual, prior to allowing access to a system, such as a workstation, laptop, server, etc.	
<b>IA-2 Identification and Authentication (Organizational Users)</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	For access to any IT asset by organizational users (including contractors), a contractor shall require identification and authentication to access this asset.	

Control# and Name	#	Control Description	Control Implementation
	02	Authentication shall be accomplished using methods such as multifactor solutions, or biometrics. A variety of multifactor solutions (including those with replay resistance) using tokens and biometrics are commercially available. Such solutions may employ hard tokens (e.g., smartcards, key fobs, or dongles) or soft tokens to store user credentials.	
	03	Organizational users shall be assigned unique identifiers and shall use multifactor authentication to access SSA servers and devices to support the SSA.	
<b>IA-4 Identifier Management</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	Prior to issuing any user accounts, the contractor shall ensure the following: <ul style="list-style-type: none"> <li>• There is a process to validate the individual receiving accounts.</li> <li>• There is approval by management to issue the account.</li> <li>• That account names are unique.</li> <li>• That account names cannot be duplicated.</li> <li>• Maintenance of a list of authorized user accounts.</li> </ul>	
	02	On a recurring basis, contractor management shall also review accounts to ensure that the list is accurate. Activities that shall be managed include: <ul style="list-style-type: none"> <li>• Periodically reviewing all accounts to ensure the list of accounts is accurate with those assigned.</li> </ul>	

Control# and Name	#	Control Description	Control Implementation
		<ul style="list-style-type: none"> <li>Establishing a table to map account names to systems and/or applications.</li> <li>Ensuring accounts are disabled or deactivated after 120 days of non-use.</li> </ul>	
	03	It is required that account lists are accurate but are subject to SSA review. Contractor shall provide a means for SSA to review.	
	04	Information for review is to include user account name, when last used, etc.	
<b>IA-5 Authenticator Management</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	When passwords or other authenticators are issued for access to systems and/or applications, IT management shall establish a practice so that the password is received and only able to be used by the authorized individual. Group accounts are not permitted. All user identifications are to be assigned to individual users. User authenticators include, for example, passwords, multifactor solutions, tokens, biometrics, Public Key Infrastructure (PKI) certificates, and key cards. Device authenticators include, for example, certificates and passwords.	
	02	When issuing passwords, the passwords shall be issued for specific use, e.g. a specific system or application and distributed as such.	
	03	All passwords shall be delivered to the user in a secure manner.	
	04	Passwords shall never be transmitted in clear text during transmission.	



Control# and Name	#	Control Description	Control Implementation
	05	For all passwords being used, passwords shall be complex/strong passwords. A strong password contains a combination of upper and lower case alphanumeric characters, numbers, and special characters.	
	06	Passwords shall be configured so they cannot be reused.	
	07	Password changes shall remember the last 12 passwords prior to allowing reuse of the passwords.	
	08	A new password shall be changed every 30 days.	
	09	Other authenticators, including tokens and certificates shall meet requirements identified in the password management controls.	
	10	All users need to be aware of their passwords and should be used only for their sole use.	
	11	Employees shall be trained on the proper handling of individual passwords to prevent unauthorized use or modification.	
	12	Control Enhancements: (1) Password-Based Authentication The isystem, for password-based authentication enforces minimum password complexity. Passwords must contain a minimum of twelve (12) characters and must contain a combination of letters, numbers, and special characters.	
	13	The system enforces at least one special character when new passwords are created.	

Control# and Name	#	Control Description	Control Implementation
	14	The password may not be the users name or account ID.	
	15	The system encrypts passwords in storage and in transmission.	
	16	The system enforces password minimum lifetime restrictions of 1 day and 30-day maximum and prohibits password reuse for 12 generations.	
<b>IA-6 Authenticator Feedback</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	When a password or other authentication mechanism is used, the system or application shall generate non-readable characters, such as asterisks to prevent this information from being viewed by an onlooker to the system.	
	02	PIV-based credentials shall be used when technically feasible. SSA could require PIV depending on the sensitivity of the data. When applications apply to SSA PIV authentication is required for all organizations users (but can be waived at SSA discretion).	

### 10.8 INCIDENT RESPONSE (IR)

Control# and Name	#	Control Description	Control Implementation
<b>Incident Response (IR)</b>		<b>Whenever there is a compromise of SSA information, contractors shall contact SSA within one hour of detection. SSA shall work closely with SSA</b>	

Control# and Name	#	Control Description	Control Implementation
		<p><b>contractors to quickly respond to a suspected incident of unauthorized disclosure or inspection.</b></p> <p><b><u>Incident Response</u> definition:</b></p> <p>Whenever there is a compromise of SSA information, contractors shall contact SSA within one hour of detection. SSA shall work closely with SSA contractors to quickly respond to a suspected incident of unauthorized disclosure or inspection.</p> <p>An incident is a violation or suspected violation of information security policies and practices as required by this document, and implemented by your business. Types of incidents include the following:</p> <ul style="list-style-type: none"> <li>• Denial of Service - An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.</li> <li>• Malicious Code – A virus, worm, Trojan horse, or other code-based malicious entity that infects a host.</li> <li>• Unauthorized Access – A person or system, without permission, gains logical access or physical access to a network, system, application, data, or other resource.</li> <li>• Inappropriate Usage – A person violates acceptable system use policies or improperly uses SSA data.</li> <li>• Multiple Components – A single incident that encompasses two or more characteristics of other incident types.</li> </ul>	

Control# and Name	#	Control Description	Control Implementation
		<ul style="list-style-type: none"> <li>• Theft – Removal of system, data/records, on system media or paper files.</li> <li>• Loss/Accident – Accidental misplacement or loss of systems, data/records on system media or paper files</li> <li>• Disclosure of Sensitive Data –The unauthorized, inadvertent disclosure of SSA data.</li> </ul>	
<b>IR-2 Incident Response Training</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	All contractor employees shall be trained on incident response and reporting procedures at least annually to understand their responsibilities on reporting security related incidents (unless required otherwise in the contract, this can be satisfied by completing the annual security awareness training).	
<b>IR-3 Incident Response Testing and Exercises</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall annually test and/or exercise the incident response capability to ensure the policies and procedures continue to function, as intended.	
	02	At a minimum, testing shall ensure that the reporting phone numbers identified in contractor procedures are accurate.	

Control# and Name	#	Control Description	Control Implementation
<b>IR-4 Incident Handling</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	All contractors shall have a procedure in place that describes the process that shall be used in the event that an incident is detected.	
	02	Incident handling procedures shall document the process used to handle incidents, including preparation, detection and analysis, containment, eradication, and recovery.	
	03	Contractors shall routinely track and document security incidents potentially affecting the confidentiality of SSA data using an automated process or tool.	
<b>IR-5 Incident Monitoring</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall track and document all system security incidents. Examples include maintaining records about each incident, the status of the incident, and other pertinent information needed for forensics, evaluating incident details, and trend analysis.	

Control# and Name	#	Control Description	Control Implementation
<b>IR-6 Incident Reporting</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	All incidents related to SSA processing, information or systems shall be reported within one hour to the SSA	
<b>IR-7 Incident Response Assistance</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	All contractors shall have an individual (or help desk or incident response team) identified who shall provide assistance on the handling of potential security incidents.	
	02	This support individual shall have adequate training and understanding to help a contractor resume business, while providing support to contain and manage a potential security incident.	
<b>IR-8 Incident Response Plan</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned  <b>(Not in Place)</b>	01	The contractor shall develop and annually review an incident response plan that provides the high-level approach to handle incidents. The plans shall: <ul style="list-style-type: none"> <li>• Define what a reportable incident is.</li> <li>• Define the resources and management support necessary to maintain an effective incident response capability.</li> </ul>	

Control# and Name	#	Control Description	Control Implementation
		<ul style="list-style-type: none"> <li>The content of the plan shall be sufficient to enable handling and reporting of security incidents within that organization.</li> </ul>	

### 10.9 MAINTENANCE (MA)

Control# and Name	#	Control Description	Control Implementation
<b>Maintenance (MA)</b>		Maintenance ensures that all IT assets are able to be used and ensures the integrity and reliability of the equipment. All contractors, small and large, shall rely on the operation and functionality of equipment if they are to provide continued service to SSA.	
<b>MA-2 Controlled Maintenance</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall maintain a maintenance log that shall provide a journal/log of all maintenance that took place on the IT assets.	
	02	Maintenance records shall be maintained for any IT assets and include: (i) the date and time of the maintenance; (ii) name of the individual or organization performing the maintenance; (iii) a description of the maintenance performed; (iv) and a list of the equipment repaired, removed, or replaced.	

Control# and Name	#	Control Description	Control Implementation
	03	The contractor shall schedule maintenance to ensure system assets are functioning, as intended. As necessary, the contractor shall review records of routine preventative and regular maintenance (including repairs) on the components of the system in accordance with manufacturer or vendor specifications and/or organizational requirements.	
	04	Prior to removing equipment from the facility for maintenance or repair, all information is to be sanitized.	
<b>MA-3 Maintenance Tools</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	When systems environments are being used, contractor personnel shall develop, and maintain an inventory of allowed maintenance tools for that environment, software and hardware.	
	02	Maintenance tools shall be checked for malicious code before installation on system(s).	
	03	Maintenance equipment/tools with storage capabilities shall be properly sanitized prior to removal from the contractor site.	
	04	Control Enhancement:  (2) Maintenance Tools   Inspect Media	



Control# and Name	#	Control Description	Control Implementation
		The contractor checks all media containing diagnostic and tests programs for malicious code before the media are used in the system.	
<b>MA-4 Non-Local Maintenance</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	Remote maintenance and diagnostic activities are those activities conducted by an individual who is communicating through a network, using a broadband communication link, Virtual Private Network (VPN), or other communication path to access the contractor's IT assets.	
	02	Remote maintenance support shall be monitored by the contractor.	
	03	When remote maintenance is performed, the following shall be accomplished:  1) The support personnel providing remote maintenance shall create and maintain a log that shall identify all remote access and maintenance into a contractor's system;  2) The IT provider shall document and identify all tools used to provide maintenance support and;  3) The IT support shall use strong two-factor identification and authentication techniques. All network communications shall be terminated when work is completed.	

Control# and Name	#	Control Description	Control Implementation
<b>MA-5 Maintenance Personnel</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	It is required that on-site maintenance personnel be escorted by the contractor when provided access (physical or logical) to IT assets where SSA data is stored or processed.	

### 10.10 MEDIA PROTECTION (MP)

Control# and Name	#	Control Description	Control Implementation
<b>Media Protection (MP)</b>		<p>Media protection controls ensure that all removable media are adequately secured to allow for the deterrence, detection, reporting, and management of loss, theft, or destruction. An inventory should be maintained and provided to SSA, upon request that identifies all media used to store, maintain, or process SSA information.</p> <p>Any media that are used to store, maintain, or process SSA information cannot be commingled with non-SSA data. All SSA information being handled or processed by the contractor must be segregated from other work being performed either logically and/or physically.</p>	

Control# and Name	#	Control Description	Control Implementation
<b>MP-7 Media Use</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned  <b>(Not in Place)</b>	01	Removable media shall not be used to store SSA data except with explicit written permission by the SSA CO or representative.	
	02	The contractor must employ FIPS 140-2 compliant cryptographic mechanisms to protect information in storage.	
	03	In addition, for all networked computers, ensure all disk areas for all computers containing SSA information are encrypted (e.g., by using an Encrypted File System) or a similar utility to encrypt data.	
	04	SSA data must be encrypted at all times to secure for logical data removed from controlled areas.	
<b>MP-2 Media Access</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall ensure that media access is restricted to prevent physical media from being lost, stolen, or disclosed.	

Control# and Name	#	Control Description	Control Implementation
<b>MP-3 Media Marking</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	For all removable media containing SSA data, the contractor shall label all media to readily identify this as SSA provided information, requiring protection.	
	02	Media shall be labeled “SSA Proprietary Data,” unless the COR provides a different labeling designation.	
<b>MP-4 Media Storage</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	Contractors who maintain SSA information shall physically control and securely store system media within controlled areas.	
	02	When this media contains SSA information, the contractor shall maintain information in a secure locked container or filing cabinet.	
	03	When bulk volumes of information are being maintained at a contractor site, the contractor shall use automated mechanisms (key card access, biometric access, cipher locks, etc.) to restrict access to media storage areas.	
	04	Access logs shall be maintained to audit access attempts.	

Control# and Name	#	Control Description	Control Implementation
<b>MP-5 Media Transport</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall ensure all information is encrypted by authorized personnel, prior to transporting any SSA information. This includes the requirement to encrypt all backup media, systems, thumb drives, optical media, portable storage media, etc.	
	02	Cryptographic mechanisms shall be used to protect the confidentiality and integrity of information stored on digital media during the transport of the media outside of controlled areas.	
	03	The contractor shall protect system media until the media are destroyed or sanitized via the use of approved equipment, techniques, or procedures.	
	04	SSA information shall be in locked cabinets or sealed packing cartons while in transit.	
	05	Accountability shall be maintained to ensure that cabinets or cartons do not become misplaced or lost during the move.	
	06	SSA information shall remain in the custody of a contractor employee and accountability shall be maintained throughout the move.	

Control# and Name	#	Control Description	Control Implementation
<b>MP-6 Sensitive Information &amp; Media Disposal</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall media, prior to disposal or release for reuse. Media shall be destroyed by either pulverizing, or cross-cut shredding.	
	02	A log shall be maintained to provide a record of media destroyed. The log shall include; (i) the date of destruction; (ii) content of media; (iii) identifying serial number; (iv) type of media; (v) media destruction performed; (vi) personnel performing the destruction; (vii) and witnesses to the destruction.	

### 10.11 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

Control# and Name	#	Control Description	Control Implementation
<b>Physical and Environmental Protection (PE)</b>		Physical security shall be provided for a document, an item, or an area via proper planning and organization to enhance security while balancing the costs. The Minimum Protection Standards (MPS) with the objective of these standards being to prevent unauthorized access to SSA information.  Physical security shall be provided for a document, an item, or an area in a number of ways. These include, but	

Control# and Name	#	Control Description	Control Implementation
		<p>are not limited to locked containers of various types, vaults, locked rooms, locked rooms that have reinforced perimeters, locked buildings, guards, electronic security systems, fences, identification systems, and control measures. How the required security is provided depends on the facility, the function of the activity, how the activity is organized, and what equipment is available.</p> <p>Proper planning and organization shall enhance the security while balancing the costs.</p> <p>The controls are intended to protect moderate information and systems at SSA. It is not the intent of SSA to mandate requirements to those systems and/or areas that are not handling and processing SSA information.</p> <p>The Minimum Protection Standards (MPS) establish a uniform method of protecting information and items that require protecting. These standards contain minimum standards that shall be applied on a case-by-case basis. Since local factors shall require additional security measures, management shall analyze local circumstances to determine space, container, and other security needs at individual facilities. The MPS have been designed to provide management with a basic framework of minimum security requirements.</p> <p>Care shall be taken to deny unauthorized access to areas containing SSA information during duty and non-duty hours. This can be accomplished by creating restricted areas, security rooms, or locked rooms. Additionally, SSA information in any form (system printout, photocopies, tapes, notes, etc.) shall be protected during</p>	

Control# and Name	#	Control Description	Control Implementation
		<p>non-duty hours. This can be done through a combination of methods: secured or locked perimeter, secured area, or containerization.</p> <p>The objective of MPS standards is to prevent unauthorized access to SSA information.</p> <p>MPS requires two barriers to access SSA information under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Locked means that an area (or container) has a lock, and that the keys or combinations are controlled. A security container is a lockable metal container with a resistance to forced penetration, with a security lock and keys or combinations are controlled. The two barriers provide an additional layer of protection to deter, delay, or detect surreptitious entry. Protected information shall be containerized in areas where other than authorized employees shall have access after-hours.</p> <p>Using a common situation as an example, often an organization desires or requires that security personnel or custodial service workers have access to locked buildings and rooms. This shall be permitted as long as there is a second barrier to prevent access to SSA information. A security guard shall have access to a locked building or a locked room if SSA information is in a locked container. If SSA information is in a locked room, but not in a locked container, the guard or janitor shall have a key to the building but not the room.</p>	



Control# and Name	#	Control Description	Control Implementation
<b>PE-2 Physical Access Authorization</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	Designated officials or designees within the contractor’s organization shall develop, review, keep current and approve the access list and authorization credentials.	
	02	The access list to the systems and areas handling and processing SSA information shall be updated at least annually.	
<b>PE-3 Physical Access Control</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	When designating an area as restricted, it is important to ensure that management controls of the area are in place. The contractor shall control all access points to the controlled area. This shall not apply to areas officially designated as publicly accessible.	
	02	The contractor shall ensure that access is authorized and verified before granting access to areas where SSA information is stored or processed.	
	03	The contractor shall maintain an Authorized Access List (AAL) of individuals authorized for entry, and establish appropriate access control procedures.	

Control# and Name	#	Control Description	Control Implementation
<b>PE-5 Access Control for Output Devices</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall control physical access to the system devices that display SSA information or where SSA information is handled or processed to prevent unauthorized individuals from observing the display output.	
<b>PE-6 Monitoring Physical Access</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor or designee shall monitor physical access to SSA information and the systems where SSA information is stored to detect and respond to physical security incidents.	
	02	The contractor shall implement an Intrusion Detection System (IDS) capability to prevent unauthorized access, break-in, or theft of SSA data.	
	03	The contractor shall provide environmental controls to alert for potential damage to SSA data.	
	04	Physical security Intrusion Detection Systems are designed to detect attempted breaches of perimeter areas. IDS must be used in conjunction with other measures to provide forced entry protection for after-hours security. Additionally, alarms for safety (fire) and other physical hazards (water pipe breaks) are recommended.	

Control# and Name	#	Control Description	Control Implementation
	05	Alarms shall annunciate at an on-site protection console, a central station, or local police station. Physical security IDS include, but are not limited to door and window contacts, magnetic switches and motion sensors designed to set off an alarm at a given location when the sensor is disturbed.	
	06	Review physical access logs quarterly at a minimum and whenever needed.	
	07	Control Enhancements: 1) Monitoring Physical Access   Intrusion Alarms / Surveillance Equipment  The contractor monitors real-time physical intrusion alarms and surveillance equipment.	

### 10.12 PERSONNEL SECURITY (PS)

Control# and Name	#	Control Description	Control Implementation
Personnel Security (PS)		All contractor and subcontractor employees performing or proposed to perform under the contract are identified to SSA at time of award (or assignment) in order to initiate appropriate background investigations. Any personnel that are not favorably adjudicated or otherwise pose a security risk are immediately removed from performance under contracts with SSA, and suitable replacement personnel agreeable to SSA are provided.	

Control# and Name	#	Control Description	Control Implementation
<b>PS-3 Personnel Screening</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	Refer to contract clause AS-401 (which concerns acquisition and grants).	
<b>PS-4 Personnel Termination</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	Upon termination of an individual's employment, the contractor shall terminate system access, conducts exit interviews, retrieve all property and devices containing SSA information.	
	02	The SSA COR shall be notified of termination of employees to the contract.	
<b>PS-5 Personnel Transfer</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall review logical and physical access authorizations to systems/facilities when personnel are reassigned or transferred to other positions; and retain access to organizational information and systems formerly controlled by a transferred individual.  For more information contact the SSA COR or the designated representative.	

### 10.13 RISK ASSESSMENT (RA)

Control# and Name	#	Control Description	Control Implementation
<b>Risk Assessment (RA)</b>		Risk assessment controls ensure that risk can be assessed within the organization, and that appropriate mitigation controls can be implemented.	
<b>RA-3 Risk Assessment</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	For stored and processed systems environments, a risk assessment shall be conducted by the contractor to assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and systems that support the operations and assets of the agency regarding the use of SSA information.	
	02	The risk assessment results shall be reviewed annually and risk assessments are to be updated every three years or whenever there is a significant change to the system or environment in which it operates.	
<b>RA-5 Vulnerability Scanning</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	All workstations, servers, network or mobile computing devices/platforms shall undergo monthly vulnerability scanning with a Security Content Automation Protocol (SCAP) compliant tool.	
	02	Any time a contractor is using IT assets, such as a workstation, laptop, server, etc., the contractor shall ensure	

Control# and Name	#	Control Description	Control Implementation
		that there are scanning tools in place to ensure that no vulnerabilities are introduced into the environment.	
	03	The contractor shall employ a host-based anti-virus and malware detection tool, and intrusion detection software on the network. At a minimum, virus detection is required to ensure malicious software is not introduced into the environment.	
	04	The virus detection software must have a current signature file.	
	05	Whenever a contractor is using networks, including LANs or WANs, the contractor shall conduct more sophisticated network scanning methods such as Network Intrusion Detections or Host Intrusion Detection to identify and correct potential network weaknesses.	
	06	The contractor shall maintain current signature files for the intrusion detection software.	
	07	The vulnerability scanning tools used shall include the capability to readily update the list of system vulnerabilities scanned.	
	08	The vulnerability scanning tools shall be updated to be current for scanning.	
	09	These reviews shall be done monthly or when significant new vulnerabilities affecting the system are identified and reported.	
	10	When providing programming services or hosting applications or services utilized by SSA, enhanced vulnerability scanning software shall also be used on	

Control# and Name	#	Control Description	Control Implementation
		services used to support the processing of SSA information. Enhanced vulnerability scanning software is capable of inspecting source code for common security flaws and performing dynamic build testing that inspects the application for security flaws at run time.	
	11	Prior to deployment or delivery, static source code analysis and dynamic build testing shall be performed.	
	12	Enhanced vulnerability scanning shall be performed whenever changes are made and dynamic build testing shall be performed on a monthly basis.	
	13	The contractor shall conduct monthly vulnerability scanning of the network.	
	14	The output and results of monthly vulnerability scanning shall be retained for the duration of the contract and provided to the COR or auditors when requested. Scan data is to be saved 180 days. Refer to SI-3 for more information.	
	15	Control Enhancement: (5) Privileged Access  The system implements privileged access authorization to the system components for selected vulnerability scanning activities. Network scanning shall not be permitted, except with network user accounts that have privileged account authority, using authorized vulnerability scanning software.	

### 10.14 SYSTEM AND COMMUNICATIONS PROTECTION (SC)

Control# and Name	#	Control Description	Control Implementation
<b>System and Communications Protection (SC)</b>		A secure system communication ensures that information is protected from unauthorized disclosure or tampering during transit, and ensures that the network communication paths, where IT assets are being used to transmit SSA information, are protected.	
<b>SC-2 Application Partitioning</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	For all contractors who manage IT development and production application environments, the system shall physically and/or logically separate user functionality (including user interface services) from system management functionality, and ensure that the separation functions are implemented and enforced.	
	02	End user accounts shall not have access to privileged system functionality. System access accounts shall be accessed by non-user privileged accounts only.	
<b>SC-4 Information in Shared Resources</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The system prevents unauthorized and unintended information transfer via shared systems resources.	



Control# and Name	#	Control Description	Control Implementation
	02	When using a shared device that stores data in the internal memory, all passwords shall be encrypted and stored separately from the device.	
	03	Once the device is stored in a facility, it shall be reset.	
<b>SC-7 Boundary Protection</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	Any contractor who manages system environments shall ensure that all internal and external system boundaries are controlled using boundary protection mechanisms, firewalls, and gateway devices.	
	02	In addition, the contractor shall ensure management personnel monitor, control, and report all accesses made through routers or switches to prevent and detect unauthorized changes to device configurations.	
	03	Control Enhancements:  (5) Deny by Default / Allow by Exception  The system at managed interfaces denies network communications traffic by default and allows network communications traffic through authorized ports and services only.	
	04	(7) Prevent Split Tunneling for Remote Devices  The system, in conjunction with a remote device, prevents the device from simultaneously establishing all connections	

Control# and Name	#	Control Description	Control Implementation
		with the system and communicating via some other connection to resources in external networks.	
<b>SC-8 Transmission Integrity</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	Whenever information is transmitted via email application or other forum, the contractor shall ensure the integrity of the information to ensure that the same information transmitted is the same information received at the termination point.	
	02	No sensitive information or PII shall be transmitted via unsecure e-mail. E-mail content is to be protected from improper disclosure.  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). As a last resort, you may send the password in a separate email message either before or after transmitting the message with the encrypted file(s). You should 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. Do not send or forward information that requires confidentiality or protection from disclosure to non-SSA accredited mobile devices/platforms.	

Control# and Name	#	Control Description	Control Implementation
		<p>Do not send or forward PII (or other information that requires confidentiality or protection from disclosure) to a non-SSA E-mail account unless the recipient is listed as secure or the information is protected by an encrypted attachment.'</p> <p>Do not set an SSA E-mail account to automatically forward work related email to an outside (non-SSA, non-secure) address.</p> <p>Do not copy (i.e., cc or bcc) work related email to your personal non-SSA email account.</p> <p>Do not include sensitive or protected information in an e-mail reply unless the recipient has secure email or the information is protected by an encrypted attachment.</p>	
	03	<p>Agreed upon technical solutions shall be implemented to ensure secure transmissions between the contractor facility and SSA. The system must perform all cryptographic operations using FIPS 140-2 validated cryptographic modules with approved modes of operation.</p> <p>A list of NIST validated modules is available at the following link:  <a href="http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#765">http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#765</a></p> <p>Bulk file encryption can be used to support this requirement.</p>	
	04	<p>File compression products must be FIP140-2 compliant (e.g., SecureZip).</p>	

Control# and Name	#	Control Description	Control Implementation
	05	SSA requires contractors to protect and control system media during transport outside of controlled areas and restrict the activities associated with transport of such media to employees without an SSA approved interim or final background investigation.	
<b>SC-10 Network Disconnect</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	All network connections shall be disconnected upon session completion or after 15 minutes, if the session is no longer in use. This may be adjusted with explicit written justification by the SSA COR or their representative providing sufficient business justification.	
<b>SC-15 Collaborative Computing Devices</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	Collaborative computing devices shall have their remote activation capability removed/disabled. This is to prevent the device from being activated when a user is not physically present.	
	02	The collaborative computing device shall also provide an indicator to the users present that the device is active. Collaborative computing devices include, but are not limited to video and/or audio conferencing capabilities.	

Control# and Name	#	Control Description	Control Implementation
<b>SC-18 Mobile Code</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	Mobile code is software that is executed from a host machine to run scripts on a client machine, including animation scripts, movies, etc. Mobile code is a powerful computing tool that can introduce risks to the user's system. Whenever a contractor is developing or deploying the mobile code technology, this shall be identified in the contractor's security plan to SSA.	
	02	Contractors, who use mobile code, shall be subject to a source code review by SSA personnel to ensure that there is no potential risk in introducing malicious code into the contractor/user's environment.	
	03	Dynamic code analysis must be performed to mitigate any code vulnerabilities and the potential of run-time vulnerabilities.	
	04	Mobile code must be approved by the COR or designated representative and subject to code analysis.	
<b>SC-23 Session Authenticity</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The system shall provide mechanisms to protect the integrity of communications sessions by authenticating the communication source and enforcing certificate-based authentication of communication devices. A password would be needed for providing a linkage to an Active Directory service account.  This applies to contractors, who are developing or providing web-based applications.	

Control# and Name	#	Control Description	Control Implementation
<b>SC-28 Protection of Information at Rest</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	All information at rest shall be encrypted to SSA standards (The encryption of data at rest should only include strong encryption methods such as AES, RSA, and SHA-256).	
	02	The contractor shall provide a solution for key management and backup and recovery services.	

### 10.15 SYSTEM AND INFORMATION INTEGRITY (SI)

Control# and Name	#	Control Description	Control Implementation
<b>System and Information Integrity (SI)</b>		This section applies to contractors, who are developing application programs, web-based interface applications, surveys that can be completed by a user population, and other instances where input data could be manipulated, causing inaccurate information to be generated. For each control, there shall be a note on the applicability to a contractor site.	
<b>SI-2 Flaw Remediation</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place )	01	Contractors shall identify, report, and correct system flaws.	

Control# and Name	#	Control Description	Control Implementation
<input type="checkbox"/> Planned (Not in Place)			
	02	Contractors shall promptly install security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or system error handling, are also addressed expeditiously.	
	03	Contractors shall incorporate flaw remediation into their configuration management process. This allows for the required/anticipated remediation actions to be tracked and verified.	
	04	The contractor shall provide the results of vulnerability scans to SSA upon request to the COR or the technical representative.	
	05	<u>Control Enhancement:</u>  (2) Flaw Remediation   Automated Flaw Remediation Status The contractor employs automated mechanisms at least monthly to determine the state of system components with regard to flaw remediation. At varying frequencies, dependent upon current threats and identified risks as determined by users, OTSO, Office of Information Security (OIS), or other agency authoritative security professionals.	

Control# and Name	#	Control Description	Control Implementation
<b>SI-3 Malicious Code Protection</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The system and/or application programs shall implement malicious code protection that includes a capability for automatic updates. Examples of malicious code include viruses, worms, spyware, Trojan horses, etc.	
	02	The contractor organization shall routinely, at least weekly, scan the IT assets for malicious code, and identify actions that shall occur in the event malicious code is detected. Possible actions include quarantine of malicious code, eradication, etc.	
	03	Virus protection software shall be installed on all workstations, servers, or mobile computing devices.	
	04	The virus detection software shall be configured to perform automated updates on a daily basis, and perform automated scanning of all files, incoming and outgoing emails, or other network communications.	
	05	Removable media, such as USB devices, diskettes, or compact disks, shall be scanned whenever they are connected to a computing device.	
	06	Procedures shall be defined to institute malicious code detection as a centrally managed process.	
	07	In addition, the contractor shall define how updates are reviewed and applied.	



Control# and Name	#	Control Description	Control Implementation
	08	Users of the system shall not be able to bypass malicious code protection controls implemented by management.	
	09	Critical updates are to be applied within 7 days, security updates within 30 days, and regular patches within 120 days.	
<b>SI-4 System Monitoring</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	The contractor shall employ tools and techniques to monitor events on the system to detect attacks, vulnerabilities, and detect, deter, and report on unauthorized use of the system.	
	02	Contractor organizations with small IT environments, (e.g., using personal systems) shall meet the intent of this control by implementing the following antivirus and firewall protection tools to monitor and protect them from cyber-attacks: <ul style="list-style-type: none"> <li>• Automated tools for near real-time analysis.</li> <li>• Automated tools that monitor inbound and outbound communications for unusual activity.</li> <li>• Tools that provides near real time alert regarding potential compromise.</li> <li>• Automated tools that prevents users from bypassing capabilities.</li> </ul>	
	03	All contractors, including those in small company environments, shall ensure they have procured and	

Control# and Name	#	Control Description	Control Implementation
		installed software to enable vulnerability detection to take place.	
	04	The contractor shall track and document all system security incidents. Examples include maintaining records about each incident, the status of the incident, and other pertinent information needed for forensics, evaluating incident details, and trend analysis.	
	05	Control Enhancement:  (4) Inbound and Outbound Communications Traffic The system monitors inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	
<b>SI-5 Security Alerts, Advisories, and Directives</b>  <b>Implementation Status:</b> (check all that apply): <input type="checkbox"/> Implemented (In Place ) <input type="checkbox"/> Planned (Not in Place)	01	For all systems, contractors shall ensure that they receive system security alerts/advisories on a regular basis, issue alerts/advisories to appropriate personnel, and take appropriate actions as necessary.	
	02	Contractors shall define appropriate personnel within the organization who shall receive the alerts/advisories, and who have responsibilities to act on these.	

## 11.0 APPENDIX B - ACRONYMS AND ABBREVIATIONS

AAL	Authorized Access List
ATM	Automated Teller Machine
CCTV	Closed Circuit Television
CD	Compact Disc
CD-R	Compact Disc Recordable
CD-ROM	Compact Disc Read Only Memory
CD-RW	Compact Disc–Rewritable
CM	Configuration Management
COR	Contracting Officer Representative
CUI	Controlled Unclassified Information
DNS	Domain Name System
DVD	Digital Video Device
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FTP	File Transfer Protocol
IDS	Intrusion Detection Systems
IEEE	Institute of Electrical and Electronics Engineers
IP	Individual Participation and Redress
ISSH	Information Systems Security Handbook
IT	Information Technology
IV&V	Independent Verification and Validation
MAC	Media Access Control
MO	Magnetic-optic
MPS	Minimum Protection Standards
NIST	National Institute of Standards and Technology
OIS	Office of Information Systems
OMB	Office of Management and Budget
OTSO	The Office of Telecommunications and Systems Operations
PII	Personal Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PM	Program Management
POA&M	Plan of Action & Milestone
RAR	Risk Assessment Report
RDP	Remote desktop
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAP	Security Assessment Package
SAR	Security Assessment Report
SBU	Sensitive But Unclassified
SP	Special Publication

SQL	Structured Query Language
SSA	Social Security Administration
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

## 12.0 APPENDIX C – INDEX

Access .. 8, 10, 11, 12, 19, 21, 22, 23, 25, 26, 27, 31, 33, 38, 47, 55, 56, 61, 62, 63, 67, 79	Contract..... 14
Account ..... 14, 19, 20, 30	Contractor ..... i, 1, 5, 6, 7, 8, 9, 14, 44, 77
Accountability..... 10, 11, 30, 57	Control 7, 8, 9, 10, 11, 19, 20, 22, 26, 27, 29, 30, 33, 35, 36, 37, 39, 40, 41, 42, 45, 47, 51, 52, 54, 58, 61, 62, 63, 65, 67, 68, 69, 74, 75, 78, 79
Acronyms..... 79	COR ..... 7, 35, 36, 56, 64, 67, 72, 73, 75, 79
AES..... 18, 27, 74	COTR..... 7, 79
Alarms..... 63	Cryptographic ..... 57
Annually..... 37	<b>CUI</b> ..... 2, 3, 79
Application..... 68	<b>Data</b> ..... 12, 18, 47, 56
Approving ..... 19	Degauss ..... 15
Architecture..... 18	<b>Denial</b> ..... 12, 47
Archives ..... 2, 3	Designated..... 61
Assessment..... 8, 9, 10, 11, 14, 33, 65, 79	Designation ..... 10
ATM..... 79	Destruction ..... 15
Attempts ..... 23	Devices..... 27, 37, 62, 69, 72
Audit ..... 10, 20, 30, 31, 32, 33	Disclosure ..... 3, 12, 47
Authenticator..... 44, 46	Disintegration..... 15
Authorization ..... 2, 10, 11, 19, 33, 61	DNS..... 79
Authorized..... 26, 40, 61, 79	Domain..... 79
Availability ..... 3	Duties ..... 5, 21
Awareness ..... 5, 7, 10, 11, 29	DVD..... 14, 27, 79
Background..... 7	Emergency ..... 20
Backup ..... 41	Encryption..... 18, 26
Baseline..... 36	Enforcement..... 21
Behavior ..... 6	Enhancement..... 35, 52, 67, 75, 78
Boundary..... 69	Environmental..... 10, 12, 58
Budget ..... 1, 79	Exception ..... 69
Building..... 2	Executive..... 1, 2
Business ..... 41	Federal..... 1, i, 1, 2, 3, 18, 28, 79
Categorization..... 1	FedRAMP ..... 2
CD ..... 14, 27, 58, 79	FIPS..... 1, 6, 18, 26, 27, 28, 55, 71, 79
Circuit ..... 14, 79	FISMA ..... 1, 79
Circular ..... 1, 2, 3, 6	Flaw..... 74, 75
CISO ..... 18	FTI..... 2
Cloud..... 2	FTP..... 39, 79
Code ..... 10, 12, 47, 73, 76	Functions..... 22, 23
Collaboration..... 8	Government..... 6, 8, 24
Confidentiality ..... 3, 26	Handling..... 49
Configuration ..... 10, 11, 36, 37, 39, 79	Identifiable ..... 2, 79
Contingency ..... 10, 11, 41	Identifier..... 9, 10, 17, 43
Continuity ..... 41	Identity ..... 8, 26, 79
Continuous ..... 6	

IDS ..... 62, 63, 79  
 IEEE ..... 79  
 Impact ..... 38  
 Incident . 3, 6, 8, 9, 10, 12, 32, 47, 48, 49, 50  
 Incineration ..... 15  
 Information . 1, i, 1, 2, 3, 5, 7, 11, 14, 15, 17,  
 18, 19, 21, 28, 29, 33, 40, 41, 44, 58, 68,  
 74, 75, 77, 79  
 Inspect ..... 52  
 Integrity ..... 3, 11, 14, 26, 42, 70, 74  
 Inventory ..... 40  
 ISSH ..... 79  
 Jurisdiction ..... 18  
 Key ..... 11, 33, 44, 79  
 Least ..... 22, 39  
 Locked ..... 13, 58  
 Logon ..... 30  
**Loss** ..... 12, 47  
 MAC ..... 27, 79  
 Maintenance ..... 10, 12, 43, 51, 52, 53, 54  
**Malicious** ..... 12, 47, 76  
 Management... 1, 2, 7, 10, 11, 19, 20, 30, 36,  
 43, 44, 79  
 Media .. 10, 12, 15, 52, 54, 55, 56, 57, 58, 79  
 Memory ..... 79  
 Milestone ..... 35, 79  
 Mobile ..... 27, 73  
 Monitoring ..... 6, 26, 49, 62, 63, 77  
 MPS ..... 13, 58, 79  
 Multifactor ..... 12, 43, 44  
 Network ..... 18, 26, 53, 66, 67, 72, 80  
 NIST ..... 1, 18, 39, 71, 79  
 Non-Federal ..... 1, i, 17  
 Nonsecurity ..... 23  
 Notification ..... 24  
 Officer ..... 7, 18, 79  
 OIS ..... 1, 75, 79  
 OMB ..... 1, 2, 6, 79  
 Organization ..... 10, 17  
 Output ..... 62  
 Package ..... 79  
 Partitioning ..... 68  
 Password ..... 45  
 Personally ..... 2  
**Personnel** ..... 7, 10, 13, 54, 63, 64  
 PHI ..... 2

**Physical** ..... 7, 10, 12, 13, 15, 58, 61, 62, 63  
 PII ..... 2, 3, 70, 79  
 PIV ..... 8, 26, 46, 79  
 PKI ..... 44, 53, 79  
 Plan ..... 3, 8, 9, 35, 41, 50, 79  
 Planning ..... 10, 11, 41  
 POA&M ..... 35, 36, 79  
 Policies ..... 5  
 Policy ..... 11  
 Privacy ..... 1, 8, 9, 19  
 Private ..... 26, 53, 80  
 Privilege ..... 22, 30  
 Process ..... 1  
 Program ..... 2, 79  
 Property ..... 15  
 Protection .. i, 5, 7, 10, 12, 13, 14, 26, 33, 54,  
 58, 68, 69, 74, 76, 79  
 Protocol ..... 39, 65, 79, 80  
 Public ..... 44, 79  
 RAR ..... 79  
 RDP ..... 79  
 Recommendation ..... 10  
 Records ..... 2, 31  
 Remediation ..... 74, 75  
 Remote ..... 25, 53, 69, 79  
 Representative ..... 7, 79  
 Response ... 3, 8, 9, 10, 12, 31, 32, 47, 48, 50  
 Responsibility ..... 17  
 Restriction ..... 18  
 Retention ..... 37  
 Review ..... 10, 14, 31, 39, 63  
 Risk ..... 2, 7, 10, 14, 37, 65, 79  
 Rules ..... 6  
 SAR ..... 9, 79  
 SAT ..... 7  
 SBU ..... 79  
 Scanning ..... 65  
 Scans ..... 7  
 SCAP ..... 65  
 SecureZip ..... 71  
 Security ... 1, i, 1, 5, 6, 7, 8, 9, 10, 11, 13, 18,  
 19, 22, 29, 33, 34, 38, 63, 65, 75, 78, 79,  
 80  
**Sensitive** ..... 12, 47, 56, 58, 79  
 Services ..... 39  
 Session ..... 25, 73

Software .....	18, 40
SP .....	1, 10, 79
SQL.....	39, 80
SSA 1, i, 1, 2, 3, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 24, 25, 27, 28, 29, 30, 32, 33, 35, 36, 38, 40, 41, 43, 44, 46, 47, 49, 50, 51, 54, 55, 56, 57, 58, 61, 62, 63, 64, 65, 66, 68, 70, 71, 72, 73, 74, 75, 80	
SSN .....	3, 70
Standards.....	1, 13, 18, 28, 58, 79
Storage .....	56
Structure.....	10
System. 1, i, 1, 3, 7, 9, 10, 11, 14, 17, 18, 20, 22, 24, 40, 41, 55, 62, 68, 74, 77, 79	
Telephone.....	17
Termination.....	14, 25, 64
Terms .....	6


Testing.....	42, 48
Theft.....	12, 47
Tools .....	52, 77
Training.....	5, 7, 10, 11, 29, 48
Transmission.....	70
Tunneling .....	69
<b>Unauthorized</b> .....	12, 47
Unclassified.....	1, 2, 79
Usage.....	12, 47
USB.....	27, 39, 76, 80
Use .....	24, 28, 55
Validation.....	7, 79
Verification .....	7, 8, 26, 79
Virtual .....	26, 53, 80
VPN.....	18, 26, 53, 80
Vulnerability .....	65
WAN .....	18, 80
Wireless.....	27





**Social Security Administration**  
Office of Information Security  
SSA Publication No. 02-010  
November 2015

*Produced and published at U.S. taxpayer expense*

 Printed on recycled paper