Controlled Unclassified Information

Enhanced Direct Enrollment Entity Name (Acronym)

Enhanced Direct Enrollment System Security and Privacy Plan

Prepared by: <Auditor Name>

For: <Name of Enhanced Direct Enrollment Entity>

<Name of Information System>

EDE SSP Version 0.1

SSP Report Publication Date

CMS SSP Template v 2.0

Introduction and Overview

The Centers for Medicare & Medicaid Services (CMS) is responsible for implementing many provisions of the health insurance reform law, the Patient Protection and Affordable Care Act of 2010 (hereafter referred to as the "Affordable Care Act" or "ACA"). To facilitate and enhance the eligibility determination and enrollment processes, CMS will provide centralized and standardized business and technical services ("Hub Web Services") through an application programming interface (API) to the Federally Facilitated Exchange (FFE) Partner, including Enhanced Direct Enrollment (EDE) Entities. This will enable the FFE Partner to establish a secure connection to the CMS Data Services Hub (Hub). The API will enable the secure transmission of key eligibility and enrollment information between CMS and the FFE Partner.

Protecting and ensuring the confidentiality, integrity, and availability (CIA) of Health Insurance Exchange (hereafter simply the "Exchange") information, common enrollment information, and associated information systems is the responsibility of the Exchange and all of its business partners. CMS is responsible for providing business, information, and technical guidance; creating common baselines and standards for information technology (IT) system implementation activities; and maintaining oversight of the FFE and IT systems that support the Exchange and common enrollment IT systems. FFE partners are considered Non-Exchange Entities (NEE) according to 45 CFR § 155.260 (b)(1) and as such are required to comply with the privacy and security standards consistent with 45 CFR § 155.260(a)(1) - (6), including being at least as protective as the standards the Exchange has established and implemented for itself under 45 C.F.R. § 155.260(a)(3).

Purpose

This document provides the System Security Plan (SSP) template for each FFE Partner Entity (Partner) responsible for implementing comprehensive security and privacy controls specified in ACA regulations. This document is intended to be used by Partners who are applying for an authorized connection to the Hub and access to consumer data contained within the Exchange repositories. Partners are required to complete the SSP and document their compliance with mandates of the ACA legislation and Department of Health and Human Services (HHS) regulations. The SSP is the key tool for describing a Partner's IT systems and supporting application(s) security and privacy environment and for documenting the implementation of security and privacy controls for the protection of all data received, stored, processed, and transmitted by the ACA support IT systems and supporting applications. The SSP must be initiated during the initial stages of the life cycle process for IT systems.

This document is released in template format. Once populated with content, it should include detailed information about Partner information security and privacy controls.

The SSP should be reviewed and updated on an as-needed basis, at least annually, and when there are major system modifications that could potentially impact the security and privacy of the Partner's information system.

Basic Assumptions about SSP for ACA FFE Partner Systems

The preparer of the System Security and Privacy Plan should consider the following basic assumptions about the Partner systems environment and the roles and responsibilities of various parties:

1. **Personally Identifiable Information (PII).** All systems will be processing ACA-related PII.
2. **Outsourcing and Cloud environments.** Most of the systems will be hosted in an outsourced computing facility or cloud environment. In many cases, the Partner will not be the service provider; accordingly, Implementation of Control statements like "The organization …" can involve multiple parties.
3. **Systems Development Life Cycle (SDLC).** All systems will be required to follow an organization-specific SDLC process. The supporting attachments includes a list of artifacts and agreements required throughout this life-cycle process.
4. **Terminology.** The following includes definitions of terms used throughout the SSP:
   - The "organization" is used generally to mean single or multiple parties on the Partner side, including the Partner or outsourced service provider. Whenever a Partner uses the term "organization," it is essential to specify the implementer.
   - The "Service Provider" is the party that provides the development and/or operational support of a component of the information technology (IT) system.
   - The "System Owner" is specifically the person in the Partner organization responsible for all IT aspects of this system [see example of usage in AC-6(1)] including the operation and maintenance of an information system. This individual can also be the IT manager/owner of the general support system (GSS).
   - A "general support system" is an interconnected set of information resources under the same direct management control that shares common functionality. A GSS normally includes hardware, software, information, applications, communications, data, and users.
   - The "System Maintainer/Developer" is the individual or group of individuals that has the responsibilities of continued maintenance (e.g., bug fixing, minor modifications / enhancements, performance tuning, and/or customer service) of an implemented system. A system maintainer may or may not also serve as the system developer for a given project.
   - The "Business Owner" is the person in the Partner organization who is responsible for the mission and ensures the system serves the business needs of the Partner.

Completing the SSP

Instruction: A completed SSP must provide detailed technical information about the system, describe the sensitive information the system processes or maintains, and demonstrate that effective security and privacy controls have been implemented to ensure protection against all known vulnerabilities. The SSP must also document the policies, processes, and procedures that are associated with the Partner organization, both at the program and system levels. Every SSP must be dated, and every page in the SSP must display the date, version number, page number, and total number of pages to facilitate review and tracking of modifications and approvals.

To complete this template, and to prevent any unnecessary processing delays, please provide the specific data requested in all associated tables and the various summary discussion sections.

Those sections that require summary information or detailed discussions of processes, policies, technical implementations, or other system-related information are preceded by "[Click here and type text]." A detailed set of instructions in blue font follows, providing the required level of specificity. Please complete the necessary summary paragraphs in the spaces provided "[Click here and type text]" and then use the instructions that follow as a checklist to ensure that all necessary requirements are addressed. Once all necessary information has been annotated in the summary paragraph(s), delete the provided instructions.

In a similar fashion, diagrams and other graphical display requests will be annotated with "[Click here to include system diagram]" or other similar text. Additional diagrams, flowcharts, or tables may be added at the author's discretion to properly describe essential components of the system, data flows, or organizational structures.

The guidance in this document helps standardize the effort of the System Developer/Maintainers, Business Owners, security and privacy officers, or equivalents in creating SSPs for the Partner Systems. The SSP identifies the following:

- Applicable laws and/or regulations affecting the system;
- The Rules of Behavior (RoB) associated with the system;
- High- and moderate-level risks identified during the risk assessment;
- Security and privacy in all levels of development;
- Personnel responsible for oversight, development, and the security and privacy of the system;
- Business process(es) associated with the system;
- The system environment;
- System interconnections;

- System security level; and
- Detail control implementation information.

Common and Hybrid Controls

Instruction: All primary direct enrollment entities and upstream entities are held to the same set of security and privacy requirements that are documented in the EDE SSP. The primary EDE entity provides many services (with requisite controls implemented) that will be used by upstream EDE entities. A primary EDE entity must supply an SSP that identifies all "common" controls and "hybrid" controls it offers. The following instructions should guide your completion of identifying all "common" controls and "hybrid" controls that a primary EDE entity must supply to an upstream EDE entity. Those "common" controls and "hybrid" controls that can be leveraged by an upstream EDE entity should be documented in the control implementation description.

[Delete this and all other instructions from your final version of this document.]

Common Controls are security or privacy controls whose implementation results in a security or privacy capability that is inheritable by multiple information systems being served by the primary EDE entity. Security control inheritance defines a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. For example, the information systems hosted in a data center will typically inherit numerous security controls from the hosting provider, such as, physical and environmental security controls or network boundary defense security controls.

The benefit of common controls is to eliminate the need for the redundant development and operation of security and privacy controls by multiple system owners, thus maximizing the use of an existing solution and minimizing the duplication of effort and reduce cost.

It is possible for an information system to inherit just part of a control from a primary EDE entity, with the remainder of the control provided by the upstream EDE entity. This is referred to as a *Hybrid Control*. In this situation, both the primary EDE entity and the upstream EDE entity have a shared responsibility of implementing the full control objectives and implementation standards.

For an EDE entity to inherit a particular security or privacy control that is implemented by the primary EDE entity, the following must be true:

- The primary EDE entity has designated the control as inheritable by documenting it in the EDE SSP implementation description as "inheritable common control" or "inheritable hybrid control"; and

- The primary EDE entity has received Request To Connect (RTC) approval from CMS and has evidence that the control is in fact operational with no major security weakness findings.

Responsibility for implementing the following -1 control families (policies and procedures) cannot be inherited and must be described in some way by the upstream EDE entity:

- AC-1, Access Control
- AT-1, Awareness and Training
- CA-1, Security Assessment and Authorization
- CP-1, Contingency Planning
- IR-1, Incident Response
- PS-1, Personnel Security

How to Complete the Security and Privacy Controls Sections of the SSP Workbook

Instruction: The following instructions should guide your completion of the comprehensive implementation description of security and privacy controls. While control guidance is not provided, the organization should leverage the most current NIST SP 800-53 for supplemental guidance.

- Describe how the security and privacy controls are implemented for all control families within the SSP.
- Discuss in detail the strategy used in implementing the controls.
- Include in the Configuration Management (CM) control section the baseline security configurations of the system/application.
- Document the organizational component or contractor who is responsible for supporting and maintaining the control.

Throughout this SSP, policies and procedures must be explicitly referenced (title and date or version) to clearly identify the document referenced. Section numbers or similar mechanisms should allow the reviewer to easily find the reference.

For applications and platforms that are leveraging/inheriting controls at the infrastructure level (or anything lower in the stack), the implementation description must simply say “inherited.” The assessor must verify that inherited controls are in place.

Note that “-1” Controls (AC-1, AU-1, SC-1, etc.) cannot be inherited and must be described in some way by the system component service provider.

[Delete this and all other instructions from your final version of this document.]

Responding to Controls

Instruction: Each control within the SSP is designed to document and explain specific procedural, technical, and policy protections that have been applied to a specific system. As each control is documented, a detailed picture should emerge and accurately reflect the security strategy that is employed to ensure the confidentiality, integrity, and availability of both the sensitive data a system processes, and the resources that are deemed essential to its sustained operation. Three primary fields comprise each control and include:

- **Control.** This field establishes the specific requirement(s) that must be met. For instance, Security Control AC-1 establishes a standard that requires written Access Control policies and procedures that specifically address carefully prescribed requirements (and also requires their review every three years).
- **Related Control Requirements.** This field identifies any control requirements that may address similar issues and can prove useful when verifying consistency in the application of security and privacy controls across the organization.
- **Control Implementation Description.** This field must be completed by the SSP author to demonstrate compliance with the specific standards established in the initial Control field. The author should clearly reference specific policies by name and then demonstrate to the assessment team that the referenced policy and/or procedures meet both the intent and the actual, specified requirements (such as a policy that addresses purpose, scope, roles, and responsibilities, etc.) The policy and procedures must also be reviewed at the required frequencies to ensure that the content is accurate and current.

[Delete this and all other instructions from your final version of this document.]

Responding to Control Implementation Descriptions

Instruction: When completing control implementation description fields, address the following:

Identify the Control Status

Instruction: It is required that you indicate the status of the control you are documenting in the Control Implementation Description field. There may be multiple control statuses within a control response if there are multiple responsible entities, or a different implementation status for different control objectives or implementation standards.

Indicate the current "**Control Status"** with one of the following:

- **Implemented** – System provides control that mitigates vulnerability/threat.
- **Inherited** – Control implementation is provided by outside source other than system (i.e., GSS, physical security, SOC/NOC, etc.).

- **Compensated** – System implements an equivalent security capability or level of protection for the information system to mitigate vulnerability/threat.
- **Planned** – Control is not implemented and actions are planned to mitigate vulnerability/threat. Security and privacy controls that are planned should be documented in the Plan of Action and Milestones (POA&M).
- **Not Applicable (N/A)–** The control does not directly apply to the information system. The system either does not perform the functions described by the controls, or the system does not employ technology under threat. **Note:** If a control is N/A, please indicate why it is N/A.

Who Is Responsible for Implementing the Solution?

Instruction: Explain who is responsible for each control implementation. The term "organization defined" must be interpreted as being the Partner's responsibility unless otherwise indicated (such as third-party service provider). In some cases, CMS has chosen to define or provide parameters, in others they have left the decision up to the Partner. In the implementation of many controls, multiple organizations (or parties, persons, or entities) may bear some responsibility. For instance, some security functionality may be outsourced to a subcontractor, while a Partner employee or organization handles other elements of the same control.

What Is the Solution? Does the Solution Satisfy the Control Requirements?

Instruction: Provide a detailed description of the solution implemented for the control. Ensure that all stated control requirements and implementation standards are addressed. The solution documented in the Control Implementation Description must satisfy each of these requirements. If the solution does not fully address each control requirement, document any compensating controls in place that reduce the residual risk.

How Often Is the Control Reviewed and by Whom?

Instruction: Please provide the review interval at the end of your Control Implementation Description. Also indicate the individual or party (by title) responsible for the review (e.g., "The IT Security Program Policy is reviewed and updated annually by the Security Officer.").

Additional Considerations for Describing Control Implementation

When documenting control implementations, it is important to provide as much detail as possible to fully describe how all aspects of the control have been addressed. In describing the control:

- Describe in detail how the control is implemented either through process, policy, or technical implementation; it is not enough to state a control is in place.

- If automated tools are utilized, describe the tool and how it satisfies the control requirement.
- Identify for each control who or what role is responsible for its implementation, and how often the control is reviewed to ensure it is working as intended.
- Attach maintenance, visitor, audit logs, and Rules of Behavior documentation as evidence of control implementation, if necessary.
- Include the title, version, and date when referencing policy documentation. Also identify the documentation's location, method of distribution, and how often policies and procedures are reviewed and by whom.

Sample Control Implementations

The following controls in Table Instr-1-1 and Table Instr-1-2 have sample responses that have been entered in the **Control Implementation Description** field using the appropriate format. Please refer to these samples as you document your Control Implementation Description.

[Delete this entire section of instructions from your final version of this document.]

Table Instr-1-1. Sample 2 – CM-4: Security Impact Analysis (Sample Response)

CM-4: Security Impact Analysis
Control
The organization analyzes changes to the information system to determine potential security and privacy impacts prior to change implementation. Activities associated with configuration changes to the information system are audited. **Implementation Standards** 1. A security and privacy impact analysis is recommended as part of change management.
Related Control Requirement(s): CA-2, CA-7, CM-3, CM-9, SA-5, SA-10, SI-2
Control Implementation Description: SAMPLE **EDE Entity IT Department** **Control Status: Implemented and Inheritable Common Control** The EDE Entity facility team maintains a site scan system that monitors the temperature and humidity in the computer room. The HVAC is monitored daily by internal staff / personnel who receive alarms in the command center when the system varies outside of set parameters. If EDE Entity customer requires a change that may impact security, a joint meeting is set up between the EDE Entity IT Department and the customer to discuss the impact before proceeding with the change. In addition, both parties agree on the correct data categorization rating (low, medium/moderate or severe) for that particular touch point. Activities associated with the change implementation are documented in the Change Ticket and can be audited if needed. Changes to configurations controlled by the INSUR System including those associated with security controls for interfaces and core INSUR middleware are fairly static. Audits are not conducted for any given interval by the EDE Entity IT Department. The service providers HB Systems and ABC Data Center are responsible for configuration change control for hardware, OS, boundary protection devices.

CM-4: Security Impact Analysis
Contractor: HB Systems **Control Status: Planned** HB Systems is in the process of implementing a formal security analysis process as part of change control. Refer to POA&M item# 37. **Data Center: ABC Data Centers** **Control Status: Implemented** A security review and approval by the client and ABC Data Centers is required prior to implementation of all changes per the EDE Entity IT Department Change Management Process. An audit of this process is performed annually by the EDE Entity IT Department for all state and contractors supporting the INSUR System.

Table Instr-1-2. Sample 3 – AR-5: Privacy Awareness and Training (Sample Response)

AR-5: Privacy Awareness and Training
Control
The organization: a. Develops, implements, and updates a comprehensive privacy training and awareness strategy aimed at ensuring personnel understand privacy responsibilities and procedures; b. Administers basic privacy training no less often than once every three hundred sixty-five (365) days, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII no less often than once every three hundred sixty-five (365) days; and c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements no less often than once every three hundred sixty-five (365) days. **Implementation Standards:** 1. A privacy education and awareness training program must be developed and implemented for all employees and individuals working on behalf of the organization involved in managing, using, and/or processing PII. 2. Privacy education and awareness training must include responsibilities associated with sending PII in email. 3. Communications and training related to privacy and security must be job-specific and commensurate with the employee's responsibilities. 4. Agencies must initially train employees (including managers) on their privacy and security responsibilities before permitting access to organization information and information systems. Thereafter, agencies must provide at least annual refresher training to ensure employees continue to understand their responsibilities. 5. Additional or advanced training must be provided commensurate with increased responsibilities or change in duties. 6. Both initial and refresher training must include acceptable rules of behavior and the consequences when the rules are not followed. 7. Training must address the rules for telework and other authorized remote access programs.

AR-5: Privacy Awareness and Training
Related Control Requirement(s): AT-2, AT-3, AT-4, TR-1
Control Implementation Description: SAMPLE **Control Status: Inherited and Interiable Hybrid Control** The Organizational Privacy Coordinator in conjunction with the Information Systems Security Officer has developed a comprehensive training and awareness program that includes the following: 1. Requirement for all users and managers to complete awareness training on an annual basis. The training includes an overview of privacy protection policies and procedures, privacy definitions, privacy technical and operational safeguards, overview of the incident response process that includes how to detect and report privacy incidents and to who, and common security threats and mitigation strategies. 2. Requirement for all new staff to complete training prior to granting access authorization to IT information systems and networks. 3. Based on notifications from Human Resources of all positions performing more specific security and privacy related responsibilities a requirement to obtain specific security and privacy training that includes real-world scenarios related to best practices for protecting PII through understanding how security and privacy principles are applied to specific job responsibilities such as Help Desk operators, security administrators, and privacy officers. These courses are required every three years 4. All training is automatically recorded and tracked on the training website that is maintained by Human Resources.
Assessment Procedure:
Assessment Objective Determine if: 1. The organization develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring personnel understand and accept AE privacy responsibilities and procedures; 2. The organization administers basic privacy training within every 365 days, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII within every 365 days; and 3. The organization ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements within every 365 days.
Assessment Methods and Objects **Examine:** 1. Organization's training and awareness policies and organization's training and awareness program plan strategy procedures describing substance and frequency of AE privacy training; 2. Privacy and awareness training materials; and 3. Records of personnel who certified completion of training. **Interview:** 1. Organization's designated privacy official and/or chief privacy officer; and 2. Other organizational personnel, as designated by privacy official, with responsibility for AE privacy training and outreach.

[Delete this entire section of instructions from your final version of this document.]

System Security Plan

Prepared by: <Identify organization that prepared this document, if not the <Non-Exchange Entity Organization>

Organization Name: <Enter Company/Organization>.

Street Address: <Enter Street Address>

Suite/Room/ Building: <Enter Suite/Room/Building>

City, State Zip: <Enter Zip Code>

Prepared for <Identify Non-Exchange Entity Organization>

Organization Name: <Enter Company/Organization>.

Street Address: <Enter Street Address>

Suite/Room/Building: <Enter Suite/Room/Building>

City, State Zip: City, State <Enter Zip Code>

Record of Changes

Date	Description
<Date>	<Revision Description>

Revision History

Date	Description	Version of SSP	Author
<Date>	<Revision Description>	<Version>	<Author>
<Date>	<Revision Description>	<Version>	<Author>

How to contact us

For questions about this document including how to use it, contact directenrollment@cms.hhs.gov.

Table of Contents

List of Tables

List of Figures

System Security Plan Approvals

Signatures of Non-Exchange Entity Organization System Authorizing Official(s) are required below.

Name	<Enter Name>	Date	<Select Date>
Title	<Enter Title>		
	Non-Exchange Entity		

Name	<Enter Name>	Date	<Select Date>
Title	<Enter Title>		
	Non-Exchange Entity		

Name	<Enter Name>	Date	<Select Date>
Title	<Enter Title>		
	Non-Exchange Entity		

1. Information System Name/Title

This System Security and Privacy Plan provides an overview of the security and privacy requirements for the <Information System Name> (<Information System Abbreviation>) and describes the controls in place for implementation to provide a level of security and privacy appropriate for the information to be transmitted, processed or stored by the system. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the <Information System Abbreviation> information system.

The security and privacy safeguards implemented for the <Information System Abbreviation> system meet the policy and control requirements set forth in this System Security and Privacy Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

Table 1-1. Information System Name and Title

Official Information System Name	Information System Abbreviation
<Information System Name>	<Information System Abbreviation>

2. Information System Categorization

The overall information system sensitivity categorization is the same as that determined for the FFE System (A system sensitivity categorization for the FFE has been performed following the FIPS 199 process) and recorded in Table 2-1. Security Categorization that follows.

Table 2-1. Security Categorization

System Sensitivity Level
Moderate (M)

The overall information system privacy categorization is the same as that determined for the FFE System and recorded in Table 2-2, Privacy Categorization that follows:

Table 2-2. Privacy Categorization

PII Confidentiality Impact Level
Moderate (M)

2.1 Security Objectives Categorization

Through review and analysis, it has been determined that the baseline security categorization for the <Information System Abbreviation> system is listed in Table 2-2.

Table 2-2. Baseline Security Configuration

<Information System Abbreviation> Security Categorization
Moderate (M)

Using this categorization, in conjunction with the risk assessment and any unique security requirements, we have established the security controls for this system, as detailed in this SSP.

2.2 E-Authentication Determination

The e-Authentication information may be found in section: Attachment 3 – E-Authentication Worksheet.

Note: Refer to NIST SP 800-63, *Digital Identity Guidelines*, for more information on e-Authentication.

3. Information System Owner

The following individual is identified in Table 3-1 as the system owner or functional proponent/advocate for this system.

Table 3-1. Information System Owner

Information System Owner Information	Detail
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

4. Authorizing Official

Instruction: The Authorizing Official is the official designated by the Partner organization, which is responsible for the security and privacy of this system.

Partner Authority to Operate (ATO): Partner Authorizing Official name, title and contact information.

[Delete this and all other instructions from your final version of this document.]

The Authorizing Official (AO) or Designated Approving Authority (DAA) for this information system is the <Insert AO information as instructed>.

Table 4-1. System Authorizing Official

System Authorizing Official Information	Detail
Name	<Enter Name>

System Authorizing Official Information	Detail
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

5. Other Designated Contacts

Instruction: AOs should use the following section to identify points of contact that understand the technical implementations of the identified system. AOs should edit, add, or modify the contacts in this section as they see fit.

[Delete this and all other instructions from your final version of this document.]

The following identified individual(s) possess in-depth knowledge of this system and/or its functions and operation.

Table 5-1. Information System Management Point of Contact

Information System Management POC	Detail
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Table 5-2. Information System Technical Point of Contact

Technical POC	Detail
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Instruction: Add more tables as needed.

[Delete this and all other instructions from your final version of this document.]

6. Assignment of Security and Privacy Responsibility

The Partner Organization Information System Security Officer (ISSO), or equivalent, identified in Table 6-1, has been appointed in writing and is deemed to have significant cyber and operational role responsibilities.

Table 6-1. Non-Exchange Entity Name Internal ISSO (or Equivalent) Point of Contact

NEE Internal ISSO	Detail
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

The Non-Exchange Entity Organization Information System Official for Privacy, named in Table 6-2, has been appointed in writing and is deemed to have significant privacy operational role responsibilities.

Table 6-2. Non-Exchange Entity Internal Official for Privacy (or Equivalent) Point of Contact

NEE Internal Official for Privacy POC	Detail
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

The CMS Information System Security Officer responsible for providing assistance to the FFE Partner security and privacy officers is named in Table 6-3.

Table 6-3. CMS ISSO Point of Contact

CMS ISSO POC	Detail
Name	CMS ISSOs
Title	ISSO
Company / Organization	CMS
Address	7500 Security Blvd., Baltimore, MD 21244-1850
Email Address	directenrollment@cms.hhs.gov

7. Information System Operational Status

The system is currently in the life-cycle phase shown in Table 7-1 that follows. (Only operational systems can be granted an RTC).

Table 7-1. System Status

Check	Status	Description
☐	Operational	The system is operating and in production.
☐	Under Development	The system is being designed, developed, or implemented
☐	Major Modification	The system is undergoing a major change, development, or transition.
☐	Other	Explain: Click here to enter text.

Instruction: Select as many status indicators as apply. If more than one status is selected, list which components of the system are covered under each status indicator.

[Delete this and all other instructions from your final version of this document.]

8. Information System Type

This section is to be used only for Non-Exchange Entities that have systems or a portion of their systems operating in a cloud environment. The <Information System Abbreviation> makes use of unique managed service provider architecture layer(s).

8.1 Cloud Service Models

Information systems, particularly those based on cloud architecture models, are made up of different service layers. Table 8-1 indicates the layers of the <Information System Abbreviation> defined in this SSP.

Instruction: Check all layers that apply.

[Delete this and all other instructions from your final version of this document.]

Table 8-1. Service Provider Architecture Layers Represented in this SSP

Check	Service Provider	Service Type
☐	Software as a Service (SaaS)	Major Application
☐	Platform as a Service (PaaS)	Major Application
☐	Infrastructure as a Service (IaaS)	General Support System
☐	Other	Explain: Click here to enter text.

Note: Refer to NIST SP 800-145 for information on cloud computing architecture models.

9. General System Description

This section includes a general description of the <Information System Abbreviation>.

9.1 System Function or Purpose

Instruction: In the space that follows, describe the purpose and functions of this system.

[Delete this and all other instructions from your final version of this document.]

9.2 Description of the Business Process

Instruction: Provide a brief description of the business process as it is supported by the system.

- **Describe the business function for each system.** Provide information regarding the overall business processes, including any business process diagrams and/or workflow diagrams.
  - Describe the underlying business processes and resources that support each business function. This may include the required inputs (business functions/processes that feed this function), processing functions (calculations, etc.), organizational/personnel roles and responsibilities, and expected outputs/products (that may "feed" other business functions / processes).
  - Describe how information flows through/is processed by the system, beginning with system input through system output. In addition, describe, for example, how the data/information is handled by the system (is the data read, stored, and purged?).

[Delete this and all other instructions from your final version of this document.]

"[Click here and type text; include diagrams as necessary]"

9.3 Information System Components and Boundaries

Instruction: In the space that follows, provide an explicit definition of the system's Authorization Boundary. Provide a diagram that portrays this Authorization Boundary and all its connections and components, including the means for monitoring and controlling communications at the external boundary and at key internal boundaries within the system.

Address all components and managed interfaces of the information system authorized for operation (e.g., routers and firewalls).

Formal names of components as they are known at the service provider organization in functional specifications, configuration guides, other documents, and live configurations shall be named on the diagram and described. Components identified in the Boundary diagram should be consistent with the Network diagram and the inventory(ies). Provide a key to symbols used. Ensure consistency between the boundary and network diagrams and respective descriptions (Section 9.5) and the appropriate Security Controls [AC-20, CA-3(1)].

[Delete this and all other instructions from your final version of this document.]

A detailed and explicit definition of the system authorization boundary diagram is represented in Figure 9-1, Authorization Boundary Diagram.

Insert picture here (styled as "Figure")

Figure 9-1. Authorization Boundary Diagram

9.4 Types of Users

All personnel have their role categorized with a sensitivity level in accordance with PS-2. Personnel (employees or contractors), including those of service providers, if applicable, are considered Internal Users. All other users are considered External Users. Table 9-1 describes Internal User privileges (authorization permission is granted after authentication takes place).

> **Instruction:** For an External User, write "Not Applicable" in the Sensitivity Level Column. This table must include all roles, including systems administrators and database administrators as role types. (Also, include web server administrators, network administrators, firewall administrators, and third-party administrators if these individuals have the ability to configure a device or host that could impact the Partner service offering.) Describe different user roles and associated levels of access to system-related data (read-only, alter, etc.), system-related facilities, and information technology resources. The first three shaded rows of Table 9-1 present examples (please delete these rows from your table).
>
> This table must also include whether these roles are fulfilled by foreign nationals or systems outside the United States.
>
> [Delete this and all other instructions from your final version of this document.]

Table 9-1. Internal Personnel Roles and Privileges

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
Example: UNIX System Administrator	Internal	P	Moderate	Full administrative access (root)	Add / remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups
Example: Client Administrator	External	NP	N/A	Portal administration	Add remote client users. Create, modify and delete client applications
Example: Program Director	Internal	NLA	Limited	N/A	Reviews, approves and enforces policy
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		

There are currently <number> internal personnel and <number> external personnel. Within one (1) year, it is anticipated that there will be <number> internal personnel and <number> external personnel.

Use Table 9-2 to provide details regarding External Users, including the following items:

- User types
- Organizations comprising the user community
- Users' level of access (e.g., read-only, alter, and the like)
- Uniform Resource Locator (URL) for web-based access
- How the system is accessed

Table 9-2. External Users

User Type (Group or Role)	Internal / External	Access Rights (Read, Write, Modify, Delete	Data Type Accessed	Expected Output / Product	User Interface (How system accessed – TCP/IP, Dial, SNA, etc.)	Web-Based Access (Provide URL)	Comments
Example: Agents / Brookers	External	R/W/D	Consumer PII for Open Enrollment		API	https://www.edeapp.com/	Singlefactor username and password authentication; two-factor authentication preferred.

9.5 Network Architecture

Instruction: Insert a network architectural diagram in the space that follows. Ensure that the following items are labeled on the diagram: hostnames, Domain Name System (DNS) servers, Dynamic Host Configuration Protocol (DHCP) servers, authentication and access control servers, directory servers, firewalls, routers, switches, database servers, major applications, storage, Internet connectivity providers, telecom circuit numbers, network interfaces and numbers, and Virtual Local Area Networks (VLAN). Major security components should be represented. If necessary, include multiple network diagrams.

Assessors should be able to easily map hardware, software, and network inventories back to this diagram.

[Delete this and all other instructions from your final version of this document.]

Figure 9-2 shows the logical network topology, mapping the data flow between components, and depicts the system network components that constitute <Information System Abbreviation>.

Insert picture here (styled as "Figure")

Figure 9-2. Network Diagram

10. System Environment and Inventory

Instruction: In the space that follows, provide a general description of the technical system environment. Include information about all system environments that are used, e.g., production environment, test environment, staging, or QA environments. Include the specific location of the alternate, backup, and operational facilities.

In your description, also include a reference to the system's hardware and software inventory, which should provide a complete listing of the system's components (operating systems/infrastructure, web applications / software, and databases). The system inventory should be maintained and updated annually by the Partner, as part of continuous monitoring efforts.

[Delete this and all other instructions from your final version of this document.]

11. Description of Operational / System Environment and Special Considerations

11.1 Operational Information

Instruction: Describe at a high level the anticipated technical environment and user community necessary to support the system and business functions. Include in this description any:

- Communications requirements;
- User-interface expectations; and
- Network connectivity requirements.

Be sure to indicate the physical location of the business processes and technology that will support the system.

[Delete this and all other instructions from your final version of this document.]

"[Click here and type text]"

11.2 System Information

Instruction: Provide a brief, general description of the technical aspects of the system. Include any environmental or technical factors that raise special security concerns, such as the use of Personal Digital Assistants, integrated wireless technology, etc. Describe:

- Principal hardware components.
- Principal software components.

- Principal firmware components (for security and network appliances).
- Principal encryption solutions and public key infrastructures.

[Delete this and all other instructions from your final version of this document.]

"[Click here and type text]" (System Description)

"[Click here to include the system diagram]"

Instruction: Attach the network connectivity diagram(s) that shall address the system component connections and security devices, which (1) protect the system and (2) monitor system access and system activity. Include an input/output diagram. For systems that have more than one server of the same type, only include one in the diagram; however, provide an accurate total count of servers in the supporting text description. Be sure to provide an introductory sentence(s) that describes the diagram.

Following the diagram, include text that will explain the various system components and their functionality. Be sure to annotate system components in the diagram to correlate specific graphic depictions with the information provided in the summary paragraph.

[Delete this and all other instructions from your final version of this document.]

"[Click here and type text]" (Description of System Components and Functionality)

11.3 System Environment

Instruction: Describe key aspects of the system operating environment beginning with the following key data points in Table 11-1 and conclude with a detailed discussion of the essential security support structure of the system.

Use Table 11-1 to address the following items:

- Provide a description of the system environment: If the system is maintained and/or operated by a contractor, describe (comprehensively) how the system is managed.
- If the system serves a large number of off-site users, list both the organizations and types of users (e.g., other agencies, assistors, and navigators).
- Describe all applications supported by the system, including the applications' functions and information processed.
- Describe how system users access the system (i.e., desktop, thin client). Include any information required to evaluate the security of the access.
- Describe the information / data stores within the system and security controls that limit access to the data.

- Describe the purpose and capabilities of the information system. Describe the functional requirements of the information system. For instance:
  - Are boundary protection mechanisms (i.e., firewalls) required?
  - Are support components such as web servers and e-mail required?
  - What types of access mechanisms (i.e., telecommuting, broadband communications) are required?
- Are "plug-in" methods (Mobile code; Active-X, JavaScript) required?
  - What operating system standards, if any, are required?

[Delete this and all other instructions from your final version of this document.]

Table 11-1. System Environment

System Environment	Response Data
Is the system owned or leased?	
Is the system operated by the Partner or by a support service contractor?	
If the system is maintained by support service contractor, describe comprehensively how the system is managed.	
If the system is operated by an Issuer run consolidated data center, provide the name, location and point of contact for the consolidated data center.	
Provide the hours of operation including time zone, if this is a facility where the system is hosted: e.g., 24x7, M–F 7:30 am – 5:00 pm.	
Document the approximate total number of user accounts and unique user types (i.e., researchers, programmers, administrative support, caseworkers, and public-facing employees).	• XX Administrator accounts • XX Programmer accounts • XX Caseworker accounts • Etc.

System Environment	Response Data
Identify critical processing periods (e.g., eligibility processing).	
If system serves a large number of off-site users, list both the organizations and types of users (e.g., other agencies).	
List all applications supported by the system including the applications' functions and the information processed.	
Describe how system users access the system (i.e., desktop, thin client, etc.). Include any information required to evaluate the security of the access.	

11.4 Data Flow

Instruction: In the space that follows, describe the flow of data in and out of system boundaries and insert a data flow diagram. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users. If necessary, include multiple data flow diagrams.

[Delete this and all other instructions from your final version of this document.]

Figure 11-1 represents the data flow in and out of the system boundaries.

Insert picture here (styled as "Figure")

Figure 11-1. Data Flow Diagram

11.5 Ports, Protocols, and Services

Instruction: In the column labeled "Used By", please indicate the components of the information system that make use of the ports, protocols, and services. In the column labeled "Purpose", indicate the purpose for the service (e.g., system logging, HTTP redirector, and load balancing). This table should be consistent with CM-6 and CM-7. Add more rows as needed.

[Delete this and all other instructions from your final version of this document.]

Table 12-2 lists the ports, protocols, and services enabled in this information system.

Table 11-2. Ports, Protocols, and Services

Ports (TCP / UDP) *	Protocols	Services	Purpose	Used By
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>

* Transmission Control Protocol (TCP), User Diagram Protocol (UDP)

12. System Interconnections

Instruction: By definition, system interconnection is the direct connection of two or more IT systems for the purpose of sharing information resources. Business Owners and managers should be acutely aware of, and obtain as much information as possible, regarding all potential vulnerabilities associated with system interconnections or that may result from information sharing. Strong situational awareness is essential when selecting appropriate security and privacy controls.

An Interconnection Security Agreement (ISA) with CMS is required if a system-to-system connection is made to the Hub to exchange data with CMS.

CMS ACA FFE Partner Systems should also maintain ISAs and Memoranda of Understanding (MOU) between all additional IT systems that connect to and share data or resources with the Partner System. Using Table 12-1, please describe the information sharing agreements in place that govern the data exchange. If not yet finalized, provide the status.

Provide details about all interconnections where transmissions cross the system boundary (inbound/outbound). This includes systems not governed by this security plan such as:

- Untrusted connections, including connections to the Internet, which require protective devices as a barrier to unauthorized system intrusion. Indicate if the connection is/are government-to-government, government-to-business, government-to-citizen, etc., and describe the controls to allow and restrict public access.
- Trusted connections that do not contain barrier protection devices such as firewalls. Indicate if the connection is/are government-to-government, government-to-business, government-to-citizen, etc., and discuss why the connection is trusted. Reference here and include in the SSP a copy of all MOUs, Memoranda of Agreements (MOA), Service-Level Agreements (SLA), and System Interconnection Agreements for provisioning IT security for this connectivity.

[Delete this and all other instructions from your final version of this document.]

Table 12-1 lists the interconnections for this information system.

Table 12-1. Interconnections

Organization Name / Connecting Entity	System Name	Internal / External	Interconnection Type (How system accessed – TCP/IP, Dial, SNA, etc.)	Authorized Access Agreement in Place (ISA, MOU, BPA, etc.)	Name & Title of Authorizing Management Official(s) and Date of Authorization:	Comments

Instruction: List all interconnected systems. Provide the IP address and interface identifier (eth0, eth1, eth2) for the Partner system that provides the connection. Name the external organization and the IP address of the external system. Indicate how the connection is being secured. For Connection Security indicate how the connection is being secured. For Data Direction, indicate which direction the packets are flowing. For Information Being Transmitted, describe what type of data is being transmitted. If a dedicated telecom line is used, indicate the circuit number. Add additional rows as needed. This table must be consistent with your response to subsection 14.4.3, CA-3: System Interconnections.

[Delete this and all other instructions from your final version of this document.]

Table 12-2 is consistent with your response to subsection 14.4.3, CA-3: System Interconnections.

Table 12-2. System Interconnections

SP* IP Address and Interface	External Organization Name and IP Address of System	External Point of Contact and Phone Number	Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.)**	Data Direction (incoming, outgoing, or both)	Information Being Transmitted	Port or Circuit Numbers
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>

* Service Processor

** Internet Protocol Security (IPSec), Virtual Private Network (VPN), Secure Sockets Layer (SSL)

13. Laws, Regulations, Standards, and Guidance

A summary of ACA Laws and Regulations applicable to FFE Partners is included in Attachment 12 – Laws and Regulations (subsection 15.12).

13.1 Applicable Laws and Regulations

Instruction: The information system name is a repeatable field that is populated when the Title Page is completed. If the Partner does not have additional laws and regulations that it must follow, please specify "N/A" in the table.

[Delete this and all other instructions from your final version of this document.]

Table 13-1Table 13-1 includes additional laws and regulations specific to <Information System Name>.

Table 13-1. Information System Name Laws and Regulations

Identification Number	Title	Date	Link
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>

13.2 Applicable Standards and Guidance

Instruction: The information system security and privacy standards and guidance applicable to FFE Partners are specified in the Partner Agreement and in this SSP.

The information system name is a repeatable field that is populated when the Title Page is completed. If the Partner does not have additional standards or guidance that it must follow, please specify "N/A" in the table.

[Delete this and all other instructions from your final version of this document.]

Table 13-2 includes in this section any additional standards and guidance specific to <Information System Name>.

Table 13-2. Information System Name – Standards and Guidance

Identification Number	Title	Date	Link
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>

14. Minimum Security and Privacy Controls

Security controls that are representative of the sensitivity of <Information System Abbreviation> are described in the sections that follow. Control enhancements are marked in parentheses. Table 14-1 presents a listing of the required security and privacy controls.

Table 14-1. Summary of Required Security and Privacy Controls

Control #	Security / Privacy Control Name
Access Control (AC)	
AC-1	Access Control Policy and Procedures
AC-2	Account Management
AC-2(1)	Account Management | Automated System Account Management
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts
AC-2(3)	Account Management | Disable Inactive Accounts
AC-2(4)	Account Management | Automated Audit Actions
AC-2(7)	Account Management | Role-Based Schemes
AC-2(10)	Account Management | Shared / Group Account Credential Termination
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-5	Separation of Duties
AC-6	Least Privilege
AC-6(1)	Least Privilege | Authorize Access to Security Functions
AC-6(2)	Least Privilege | Non-Privileged Access for Non-Security Functions
AC-6(5)	Least Privilege | Privileged Accounts
AC-6(9)	Least Privilege | Auditing Use of Privileged Functions
AC-6(10)	Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions
AC-7	Unsuccessful Logon Attempts
AC-8	System Use Notification
AC-10	Concurrent Session Control
AC-11	Session Lock
AC-11(1)	Session Lock | Pattern-Hiding Displays
AC-12	Session Termination
AC-14	Permitted Actions Without Identification or Authentication
AC-17	Remote Access
AC-17(1)	Remote Access | Automated Monitoring/Control
AC-17(2)	Remote Access | Protection of Confidentiality / Integrity Using Encryption
AC-17(3)	Remote Access | Managed Access Control Points
AC-17(4)	Remote Access | Privileged Commands / Access
AC-17(9)	Remote Access | Disconnect / Disable Access

Control #	Security / Privacy Control Name
AC-18	Wireless Access
AC-18(1)	Wireless Access | Authentication and Encryption
AC-19	Access Control for Mobile Devices
AC-19(5)	Access Control for Mobile Devices | Full-Device / Container-Based Encryption
AC-20	Use of External Information Systems
AC-20(1)	Use of External Information Systems | Limits on Authorized Use
AC-20(2)	Use of External Information Systems | Portable Storage Devices
AC-21	Information Sharing
AC-22	Publicly Accessible Content
Awareness and Training (AT)	
AT-1	Security Awareness and Training Policy and Procedures
AT-2	Security Awareness Training
AT-2(2)	Security Awareness Training | Insider Threat
AT-3	Role-Based Security Training
AT-4	Security Training Records
Audit and Accountability (AU)	
AU-1	Audit and Accountability Policy and Procedures
AU-2	Audit Events
AU-2(3)	Audit Events | Reviews and Updates
AU-3	Content of Audit Records
AU-3(1)	Content of Audit Records | Additional Audit Information
AU-4	Audit Storage Capacity
AU-5	Response to Audit Processing Failures
AU-5(1)	Response to Audit Processing Failures | Audit Storage Capacity
AU-6	Audit Review, Analysis, and Reporting
AU-6(1)	Audit Review, Analysis, and Reporting | Process Integration
AU-6(3)	Audit Review, Analysis, and Reporting | Correlate Audit Repositories
AU-7	Audit Reduction and Report Generation
AU-7(1)	Audit Reduction and Report Generation | Automatic Processing
AU-8	Time Stamps
AU-8(1)	Time Stamps | Synchronization with Authoritative Time Source
AU-9	Protection of Audit Information
AU-9(4)	Protection of Audit Information | Access by Subset of Privileged Users
AU-10	Non-Repudiation
AU-11	Audit Record Retention
AU-12	Audit Generation
Security Assessment and Authorization (CA)	
CA-1	Security Assessment and Authorization Policies and Procedures
CA-2	Security Assessments

Control #	Security / Privacy Control Name
CA-2(1)	Security Assessments | Independent Assessors
CA-3	System Interconnections
CA-3(5)	System Interconnections | Restrictions on External System Connections
CA-5	Plan of Action and Milestones
CA-6	Security Authorization
CA-7	Continuous Monitoring
CA-7(1)	Continuous Monitoring | Independent Assessment
CA-8	Penetration Testing
CA-8(1)	Penetration Testing | Independent Penetration Agent or Team
CA-9	Internal System Connections
Configuration Management (CM)	
CM-1	Configuration Management Policy and Procedures
CM-2	Baseline Configuration
CM-2(1)	Baseline Configuration | Reviews and Updates
CM-2(3)	Baseline Configuration | Retention of Previous Configurations
CM-3	Configuration Change Control
CM-3(2)	Configuration Change Control | Test/Validate/Document Changes
CM-4	Security Impact Analysis
CM-4 (1)	Security Impact Analysis | Separate Test Environments
CM-5	Access Restrictions for Change
CM-5(1)	Access Restrictions for Change | Automated Access Enforcement / Auditing
CM-5(5)	Access Restrictions for Change | Limit Production/Operational Privileges
CM-6	Configuration Settings
CM-6(1)	Configuration Settings | Automated Central Management / Application / Verification
CM-7	Least Functionality
CM-7(1)	Least Functionality | Periodic Review
CM-7(2)	Least Functionality | Prevent Program Execution
CM-7(4)	Least Functionality | Unauthorized Software/Blacklisting
CM-8	Information System Component Inventory
CM-8(1)	Information System Component Inventory | Updates During Installations/Removals
CM-8(3)	Information System Component Inventory | Automated Unauthorized Component Detection
CM-8(5)	Information System Component Inventory | No Duplicate Accounting of Components
CM-9	Configuration Management Plan
CM-10	Software Usage Restrictions
CM-10(1)	Software Usage Restrictions | Open Source Software
CM-11	User-Installed Software
Contingency Planning (CP)	

Control #	Security / Privacy Control Name
CP-1	Contingency Planning Policy and Procedures
CP-2	Contingency Plan
CP-2(1)	Contingency Plan | Coordinate with Related Plans
CP-2(2)	Contingency Plan | Capacity Planning
CP-2(3)	Contingency Plan | Resume Essential Missions/Business Functions
CP-2(8)	Contingency Plan | Identify Critical Assets
CP-3	Contingency Training
CP-4	Contingency Plan Testing
CP-4(1)	Contingency Plan Testing | Coordinate with Related Plans
CP-6	Alternate Storage Site
CP-6(1)	Alternate Storage Site | Separation from Primary Site
CP-6(3)	Alternate Storage Site | Accessibility
CP-8	Telecommunications Services
CP-8(1)	Telecommunications Services | Priority of Service Provisions
CP-8(2)	Telecommunications Services | Single Points of Failure
CP-9	Information System Backup
CP-9(1)	Information System Backup | Testing for Reliability/Integrity
CP-10	Information System Recovery and Reconstitution
CP-10(2)	Information System Recovery and Reconstitution | Transaction Recovery
Identification and Authentication (IA)	
IA-1	Identification and Authentication Policy and Procedures
IA-2	Identification and Authentication (Organizational Users)
IA-2(1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts
IA-2(2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts
IA-2(3)	Identification and Authentication (Organizational Users) | Local Access to Privileged Accounts
IA-2(8)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts – Replay Resistant
IA-2(11)	Identification and Authentication (Organizational Users) | Remote Access – Separate Device
IA-3	Device Identification and Authentication
IA-4	Identifier Management
IA-5	Authenticator Management
IA-5(1)	Authenticator Management | Password-Based Authentication
IA-5(2)	Authenticator Management | PKI-Based Authentication
IA-5(3)	Authenticator Management | In-Person or Trusted Third-Party Registration
IA-5(7)	Authenticator Management | No Embedded Unencrypted Static Authenticators
IA--5(11)	Authenticator Management | Hardware Token-Based Authentication
IA-6	Authenticator Feedback

Control #	Security / Privacy Control Name
IA-7	Cryptographic Module Authentication
IA-8	Identification and Authentication (Non-Organizational Users)
IA-8(2)	Identification and Authentication (Non-Organizational Users) | Acceptance of Third-Party Credentials
Incident Response (IR)	
IR-1	Incident Response Policy and Procedures
IR-2	Incident Response Training
IR-3	Incident Response Testing
IR-3(2)	Incident Response Testing | Coordination with Related Plans
IR-4	Incident Handling
IR-4(1)	Incident Handling | Automated Incident Handling Processes
IR-5	Incident Monitoring
IR-6	Incident Reporting
IR-6(1)	Incident Reporting | Automated Reporting
IR-7	Incident Response Assistance
IR-7(1)	Incident Response Assistance | Automation Support for Availability of Information/Support
IR-8	Incident Response Plan
IR-9	Information Spillage Response
Maintenance (MA)	
MA-1	System Maintenance Policy and Procedures
MA-2	Controlled Maintenance
MA-3	Maintenance Tools
MA-3(1)	Maintenance Tools | Inspect Tools
MA-3(2)	Maintenance Tools | Inspect Media
MA-3(3)	Maintenance Tools | Prevent Unauthorized Removal
MA-4	Nonlocal Maintenance
MA-4(1)	Nonlocal Maintenance | Auditing and Review
MA-4(2)	Nonlocal Maintenance | Document Nonlocal Maintenance
MA-5	Maintenance Personnel
MA-6	Timely Maintenance
Media Protection (MP)	
MP-1	Media Protection Policy and Procedures
MP-2	Media Access
MP-3	Media Marking
MP-4	Media Storage
MP-5	Media Transport
MP-5(4)	Media Transport | Cryptographic Protection
MP-6	Media Sanitization
MP-7	Media Use

Control #	Security / Privacy Control Name
MP-7(1)	Media Use | Prohibit Use Without Owner
Physical and Environmental Protection (PE)	
PE-1	Physical and Environmental Protection Policy and Procedures
PE-2	Physical Access Authorizations
PE-2(1)	Physical Access Authorizations | Access by Position / Role
PE-3	Physical Access Control
PE-4	Access Control for Transmission Medium
PE-5	Access Control for Output Devices
PE-6	Monitoring Physical Access
PE-6(1)	Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment
PE-8	Visitor Access Records
Planning (PL)	
PL-1	Security Planning Policy and Procedures
PL-2	System Security Plan
PL-2(3)	System Security Plan | Plan / Coordinate with Other Organizational Entities
PL-4	Rules of Behavior
PL-4(1)	Rules of Behavior | Social Media and Networking Restrictions
PL-8	Information Security Architecture
Personnel Security (PS)	
PS-1	Personnel Security Policy and Procedures
PS-2	Position Risk Designation
PS-3	Personnel Screening
PS-4	Personnel Termination
PS-5	Personnel Transfer
PS-6	Access Agreements
PS-7	Third-Party Personnel Security
PS-8	Personnel Sanctions
Risk Assessment (RA)	
RA-1	Risk Assessment Policy and Procedure
RA-3	Risk Assessment
RA-5	Vulnerability Scanning
RA-5(1)	Vulnerability Scanning | Update Tool Capability
RA-5(2)	Vulnerability Scanning | Update by Frequency/Prior to New Scan/When Identified
RA-5(5)	Vulnerability Scanning | Privileged Access
System and Services Acquisition (SA)	
SA-1	System and Services Acquisition Policy and Procedures
SA-2	Allocation of Resources
SA-3	System Development Life Cycle

Control #	Security / Privacy Control Name
SA-4	Acquisition Process
SA-4(1)	Acquisition Process | Functional Properties of Security Controls
SA-4(2)	Acquisition Process | Design/Implementation Information for Security Controls
SA-4(9)	Acquisition Process | Functions / Ports / Protocols / Services in Use
SA-5	Information System Documentation
SA-8	Security Engineering Principles
SA-9	External Information System Services
SA-10	Developer Configuration Management
SA-11	Developer Security Testing and Evaluation
SA-15	Development Process, Standards, and Tools
SA-17	Developer Security Architecture and Design
SA-22	Unsupported System Components
System and Communications Protection (SC)	
SC-1	System and Communications Protection Policy and Procedures
SC-2	Application Partitioning
SC-4	Information in Shared Resources
SC-5	Denial of Service Protection
SC-6	Resource Availability
SC-7	Boundary Protection
SC-7(3)	Boundary Protection | Access Points
SC-7(4)	Boundary Protection | External Telecommunications Services
SC-7(5)	Boundary Protection | Deny by Default/Allow by Exception
SC-7(7)	Boundary Protection | Prevent Split Tunneling for Remote Devices
SC-7(8)	Boundary Protection | Route Traffic to Authenticated Proxy Servers
SC-7(12)	Boundary Protection | Host-Based Protection
SC-7(13)	Boundary Protection | Isolation of Security Tools/Mechanisms/Support Components
SC-7(18)	Boundary Protection | Fail Secure
SC-8	Transmission Confidentiality and Integrity
SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection
SC-8(2)	Transmission Confidentiality and Integrity | Pre/Post Transmission Handling
SC-10	Network Disconnect
SC-12	Cryptographic Key Establishment and Management
SC-12(2)	Cryptographic Key Establishment and Management | Symmetric Keys
SC-13	Cryptographic Protection
SC-17	Public Key Infrastructure Certificates
SC-18	Mobile Code
SC-19	Voice Over Internet Protocol
SC-20	Secure Name/Address Resolution Service (Authoritative Source)

Control #	Security / Privacy Control Name
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)
SC-22	Architecture and Provisioning for Name/Address Resolution Service
SC-23	Session Authenticity
SC-24	Fail in Known State
SC-28	Protection of Information at Rest
SC-CMS-1	Electronic Mail
System and Information Integrity (SI)	
SI-1	System and Information Integrity Policy and Procedures
SI-2	Flaw Remediation
SI-2(2)	Flaw Remediation | Automated Flaw Remediation Status
SI-2(3)	Flaw Remediation | Time to Remediate Flaws / Benchmarks for Corrective Actions
SI-3	Malicious Code Protection
SI-3(2)	Malicious Code Protection | Automatic Updates
SI-4	Information System Monitoring
SI-4(1)	Information System Monitoring | System-Wide Intrusion Detection System
SI-4(4)	Information System Monitoring | Inbound and Outbound Communications Traffic
SI-4(5)	Information System Monitoring | System-Generated Alerts
SI-5	Security Alerts, Advisories, and Directives
SI-6	Security Function Verification
SI-7	Software, Firmware, and Information Integrity
SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks
SI-7(7)	Software, Firmware, and Information Integrity | Integration of Detection and Response
SI-8	Spam Protection
SI-8(2)	Spam Protection | Automatic Updates
SI-10	Information Input Validation
SI-11	Error Handling
SI-12	Information Handling and Retention
SI-16	Memory Protection
Authority and Purpose (AP)	
AP-1	Authority to Collect
AP-2	Purpose Specification
Accountability, Audit, and Risk Management (AR)	
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development

Control #	Security / Privacy Control Name
AR-8	Accounting of Disclosures
Data Quality and Integrity (DI)	
DI-1	Data Quality
DI-1(1)	Data Quality | Validate PII
Data Minimization and Retention (DM)	
DM-1	Minimization of Personally Identifiable Information
DM-1(1)	Minimization of Personally Identifiable Information | Locate / Remove / Redact / Anonymize PII
DM-2	Data Retention and Disposal
DM-2 (1)	Data Retention and Disposal | System Configuration
DM-3	Minimization of PII Used in Testing, Training, and Research
DM-3 (1)	Minimization of PII Used in Testing, Training, and Research | Risk Minimization Techniques
Individual Participation and Redress (IP)	
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
IP-4 (1)	Complaint Management | Response Time
Security (SE)	
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
Transparency (TR)	
TR-1	Privacy Notice
TR-3	Dissemination of Privacy Program Information
Use Limitation (UL)	
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Note: The -1 Controls (AC-1, AU-1, SC-1, etc.) cannot be inherited and must be provided in some way by the service provider.

Instruction: In the sections that follow, describe the information security control as it is implemented on the system. All controls originate from a system or from a business process. It is important to describe where the control originates from so that it is clear whose responsibility it is to implement, manage, and monitor the control. In some cases, the responsibility is shared by a PARTNER and by a contracted service provider. Use the definitions in the table that follows to indicate the origin of each security control. While control guidance is not provided, the organization should leverage the most current NIST SP 800-53 for

supplemental guidance.

Throughout this SSP, policies and procedures must be explicitly referenced (title and date or version) to clearly identify the document referenced. Section numbers or similar mechanisms should allow the reviewer to easily find the reference.

[Delete this and all other instructions from your final version of this document.]

14.1 Access Control (AC)

14.1.1 AC-1: Access Control Policy and Procedures Requirements

AC-1: Access Control Policy and Procedures
Control
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates (as necessary) the current: 1. Access control policy at least every three (3) years; and 2. Access control procedures at least every three (3) years.
Related Control Requirement(s): AR-4, AR-7
Control Implementation Description: «Click here and type text.]»

14.1.2 AC-2: Account Management

AC-2: Account Management
Control
The organization: a. Identifies and selects the following types of information system (IS) accounts to support organizational missions/business functions: individual, group, system, application, guest/anonymous, emergency, and temporary; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by defined personnel or roles (defined in the applicable security plan) for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with the organization requirements, standards and procedures; g. Monitors the use of information system accounts; h. Notifies account managers: 1. When accounts are no longer required;

AC-2: Account Management
2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes. i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions. j. Reviews accounts for compliance with account management requirements at least every 90 days; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. **Implementation Standards** 1. Remove or disable default user accounts. Rename active default accounts. 2. Implement centralized control of user access administrator functions. a. Regulate the access provided to contractors and define security requirements for contractors. b. Notify account managers within an organization-defined timeframe when temporary accounts are no longer required or when information system users are terminated or transferred or information system usage or need-to-know/need-to-share changes. 3. Prohibit use of guest, anonymous, and shared accounts for providing access to PII. 4. Notify account managers within an organization-defined timeframe when temporary accounts are no longer required or when IS users are terminated or transferred or IS usage or need-to-know/need-to-share changes. 5. Prior to granting access to PII, users demonstrate a need for the PII in the performance of the user's duties. 6. Implement access controls within the IS based on users' or user group's need for access to PII in the performance of their duties. 7. Organizations should provide access only to the minimum amount of PII necessary for users to perform their duties. 8. Create, enable, modify, disable, and remove information system accounts in accordance with the requirement for each user to complete privacy training every 365 days otherwise the account would be disabled.
Related Control Requirement(s): AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, CM-5, CM-6, CM-11, IA-2, IA-4, IA-5, IA-8, MA-3, MA-4, MA-5, PL-4, SC-13
Control Implementation Description: "Click here and type text"

14.1.2.1 AC-2 (1): Automated Information System Account Management

AC-2 (1): Automated Information System Account Management
Control
The organization employs automated mechanisms to support the management of information system accounts.
Related Control Requirement(s):

AC-2 (1): Automated Information System Account Management
Control Implementation Description: "Click here and type text"

14.1.2.2 AC-2 (2): Removal of Temporary / Emergency Accounts

AC-2 (2): Removal of Temporary/Emergency Accounts
Control
The information system automatically disables emergency accounts within twenty-four (24) hours and temporary accounts with a fixed duration not to exceed 60 days.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.1.2.3 AC-2 (3): Disable Inactive Accounts

AC-2 (3): Disable Inactive Accounts
Control
The information system automatically disables inactive accounts within sixty (60) days.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.1.2.4 AC-2 (4): Automated Audit Actions

AC-2 (4): Automated Audit Actions
Control
The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies defined personnel or roles (defined in the applicable security plan). **Implementation Standard** Account management information sources include systems, appliances, devices, services, and applications (including databases).
Related Control Requirement(s):

AC-2 (4): Automated Audit Actions
Control Implementation Description:
"Click here and type text"

14.1.2.5 AC-2 (7): Role-Based Schemes

AC-2 (7): Role-Based Schemes
Control
The organization: a. Establishes and administers application-specific privileged user accounts in accordance with a role-based access scheme that allows access based on user responsibilities associated with application use; b. Monitors privileged role assignments as well as application-specific privileged role assignments; and c. Takes corrective actions when privileged role assignments are no longer appropriate.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.1.2.6 AC-2 (10): Shared / Group Account Credential Termination

AC-2(10): Shared / Group Account Credential Termination
Control
The information system updates shared/group account credentials when members leave the group.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.1.3 AC-3: Access Enforcement

AC-3: Access Enforcement
Control
The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. **Implementation Standards** 1. If encryption is used as an access control mechanism, it must meet FIPS 140-2 compliant encryption standards (see SC-13).

AC-3: Access Enforcement
2. Configure operating system controls to disable public "read" and "write" access to files, objects, and directories that may directly impact system functionality and/or performance, or that contain sensitive information. 3. Data stored in the information system must be protected with system access controls and must be encrypted when residing in non-secure areas.
Related Control Requirement(s): AC-4, AC-5, AC-6, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3
Control Implementation Description: "Click here and type text"

14.1.4 AC-4: Information Flow Enforcement

AC-4: Information Flow Enforcement
Control
The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. **Implementation Standard** Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. NIST SP 800-53 control enhancements 3 through 22, while not present in this SSP workbook, provide guidance on cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial-off-the-shelf (COTS) information technology products.
Related Control Requirement(s): AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18
Control Implementation Description: "Click here and type text"

14.1.5 AC-5: Separation of Duties

AC-5: Separation of Duties
Control
The organization:

AC-5: Separation of Duties
a. Separates duties of individuals as necessary (defined in the applicable security plan), to prevent malevolent activity without collusion; b. Documents separation of duties; and c. Defines information system access authorizations to support separation of duties. d. Enforces role-based access control policies over all subjects and objects where the policy specifies that: 1. The policy is uniformly enforced across all subjects and objects within the boundary of the IS; and 2. A subject that has been granted access to information is constrained from doing any of the following: a. Passing the information to unauthorized subjects or objects; b. Granting its privileges to other subjects; c. Changing one or more security attributes on subjects, objects, the IS, or IS components; d. Choosing the security attribute and attribute values to be associated with newly created or modified objects; or e. Changing the rules governing access control. **Implementation Standards** 1. Audit functions must not be performed by security personnel responsible for administering access control. 2. Maintain a limited group of administrators with access based upon the users' roles and responsibilities. 3. The critical mission functions and information system support functions must be divided among separate individuals. 4. The information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions must be divided among separate individuals or groups. 5. An independent entity, not the Business Owner, ISSO, System Developer(s)/Maintainer(s), or System administrator(s) responsible for the information system, conducts information security testing of the information system. 6. Assign user accounts and authenticators in accordance with role-based access control policies. 7. Configure the system to request user ID and authenticator prior to system access 8. Configure databases containing federal information in accordance with the organizational security administration guide to provide role-based access controls enforcing assigned privileges and permissions at the file, table, row, column, or cell level, as appropriate.
Related Control Requirement(s): AC-3, AC-6, PE-3, PE-4, PS-2
Control Implementation Description: "Click here and type text"

14.1.6 AC-6: Least Privilege

AC-6: Least Privilege
Control
The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with the organization's missions and business functions. **Implementation Standards** 1. Disable all file system access not explicitly required for system, application, and administrator functionality.

AC-6: Least Privilege
2. Contractors must be provided with minimal system and physical access, and must agree to and support the organizational security requirements. The contractor selection process must assess the contractor's ability to adhere to and support the organization's security policy. 3. Restrict the use of database management utilities to only authorized database administrators. Prevent users from accessing database data files at the logical data view, field, or field-value level. Implement table-level access control. 4. Ensure that only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties. 5. Disable all system and removable media boot access unless it is explicitly authorized by the organization CIO for compelling operational needs. If system and removable media boot access is authorized, boot access is password protected.
Related Control Requirement(s): AC-2, AC 3, AC 5, CM 6, CM 7, PL-2
Control Implementation Description: "Click here and type text"

14.1.6.1 AC-6 (1): Authorize Access to Security Functions

AC-6 (1): Authorize Access to Security Functions
Control
At a minimum, the organization explicitly authorizes access to organization-defined list of security functions (deployed in hardware, software, and firmware) to include the following list of security functions and security-relevant information for all system components: a. Setting/modifying audit logs and auditing behavior; b. Setting/modifying boundary protection system rules; c. Configuring/modifying access authorizations (i.e., permissions, privileges); d. Setting/modifying authentication parameters; and e. Setting/modifying system configurations and parameters.
Related Control Requirement(s): AC-17, AC-18, AC-19
Control Implementation Description: "Click here and type text"

14.1.6.2 AC-6 (2): Non-Privileged Access for Non-Security Functions

AC-6 (2): Non-Privileged Access for Non-Security Functions
Control
At a minimum, the organization requires that users of information system accounts, or roles, with access to all security functions 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. This includes the following list of security functions or security-relevant information: a. Setting/modifying audit logs and auditing behavior; b. Setting/modifying boundary protection system rules;

AC-6 (2): Non-Privileged Access for Non-Security Functions
c. Configuring/modifying access authorizations (i.e., permissions, privileges); d. Setting/modifying authentication parameters; and e. Setting/modifying system configurations and parameters.
Related Control Requirement(s): PL-4
Control Implementation Description: "Click here and type text"

14.1.6.3 AC 6 (5): Privileged Accounts

AC-6 (5): Privileged Accounts
Control
The organization restricts privileged accounts on the information system to defined personnel or roles (defined in the applicable security plan).
Related Control Requirement(s): CM-6
Control Implementation Description: "Click here and type text"

14.1.6.4 AC-6 (9): Auditing Use of Privileged Functions

AC-6 (9): Auditing Use of Privileged Functions
Control
The information system audits the execution of privileged functions.
Related Control Requirement(s): AU-2
Control Implementation Description: "Click here and type text"

14.1.6.5 AC-6 (10): Prohibit Non-Privileged Users from Executing Privileged Functions

AC-6 (10): Prohibit Non-Privileged Users from Executing Privileged Functions
Control
The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
Related Control Requirement(s):

AC-6 (10): Prohibit Non-Privileged Users from Executing Privileged Functions
Control Implementation Description:
"Click here and type text"

14.1.7 AC-7: Unsuccessful Logon Attempts

AC-7: Unsuccessful Logon Attempts
Control
The information system: a. Enforces the limit of consecutive invalid login attempts by a user specified in the Implementation Standard during the time period specified in the Implementation Standard; and b. Automatically disables or locks the account/node until released by an administrator or after the time period specified in the Implementation Standard when the maximum number of unsuccessful attempts is exceeded. **Implementation Standards** 1. Enforces a limit of not more than three (3) consecutive invalid login attempts by a user during a fifteen (15) minute time; and 2. Automatically locks the account/node for thirty (30) minutes when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.
Related Control Requirement(s):
AC-2, AC 14, IA-5
Control Implementation Description:
"Click here and type text"

14.1.8 AC-8: System Use Notification

AC-8: System Use Notification
Control
The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The approved banner states: *"This warning banner applies to the entirety of this system, meaning (1) this computer network, (2) all computers connected to this network, including this one, and (3) all devices and storage media attached to this network or to a computer on this network. This system is provided for authorized [Organization name] use only. Unauthorized or improper use of this system is prohibited and may result in disciplinary action and/or civil and criminal penalties.* *By using this system, you understand and consent to the following:* *[Organization name] may monitor, record, and audit your system usage. Therefore, you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this system.* *At any time, and for any lawful purpose, [Organization name] may monitor, intercept, and search and*

AC-8: System Use Notification
seize any communication or data transiting or stored on this system. Any communication or data transiting or stored on this system may be disclosed or used for any lawful [Organization name] purpose." b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information when appropriate, before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system. **Implementation Standards** 1. The System Owner determines elements of the environment that require the System Use Notification control. 2. The System Owner determines how System Use Notification will be verified and provides appropriate periodicity of the check. 3. If not performed as part of a Configuration Baseline check, the organization has a documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.1.9 AC-10: Concurrent Session Control

AC-10: Concurrent Session Control
Control
The information system limits the number of concurrent sessions for each system account to one (1) session for both normal and privileged users. The number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties and any requirement for more than one (1) concurrent application/process session is documented in the security plan.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.1.10 AC-11: Session Lock

AC-11: Session Lock
Control
The information system: a. Prevents further access to the system by initiating a session lock after fifteen (15) minutes of inactivity (for both remote and internal access connections) or upon receiving a request from a user; and

AC-11: Session Lock
b. Retains the session lock until the user reestablishes access using established identification and authentication procedures. **Implementation Standard** Period of inactivity must be no more than 15 minutes before session lock occurs for remote and mobile devices and requires re-authentication. As organizations continue to migrate to laptops and docking stations making clients increasingly mobile, this is a logical extension of that requirement.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.1.10.1 AC-11 (1): Pattern-Hiding Displays

AC-11 (1): Pattern-Hiding Displays
Control
The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.1.11 AC-12: Session Termination

AC-12: Session Termination
Control
The information system automatically terminates a user session after defined conditions or trigger events (defined in the applicable security plan) requiring session disconnect.
Related Control Requirement(s): SC-10, SC-23
Control Implementation Description: "Click here and type text"

14.1.12 AC-14: Permitted Actions Without Identification or Authentication

AC-14: Permitted Actions Without Identification or Authentication
Control
The organization: a. Identifies specific user actions that can be performed on the information system without identification or authentication; b. Documents and provides supporting rationale in the system security plan for user actions not requiring identification or authentication; and c. Configures Information systems to permit public access without first requiring individual identification and authentication only to the extent necessary to accomplish mission objectives.
Related Control Requirement(s): CP-2, IA-2
Control Implementation Description: "Click here and type text"

14.1.13 AC-17: Remote Access

AC-17: Remote Access
Control
The organization monitors for unauthorized remote access to the information system (including access to internal networks by VPN). Remote access for privileged functions must be permitted only for compelling operational needs, must be strictly controlled, and must be explicitly authorized, in writing, by the organization CIO or his/her designated representative. If remote access is authorized, the organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; b. Authorizes remote access to the information system prior to allowing such connections; and c. Monitors for unauthorized remote access to the information system. d. Personally-owned equipment must be scanned before being connected to the organization systems or networks to ensure compliance with the organization requirements; and e. Personally-owned equipment must be prohibited from processing, accessing, or storing organization sensitive information unless it is approved in writing by the organization Senior Official for Privacy (SOP) and employs required encryption (FIPS 140-2 validated module). **Implementation Standards** 1. Require callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) or Multi-Protocol Label Switching (MPLS) service network cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor will be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems will be authorized and logged. User IDs assigned to vendors will be recertified within every three hundred sixty-five (365) days. 2. If e-authentication is implemented as a remote access solution or associated with remote access, refer to the most recent NIST SP 800-63. 3. All computers and devices, whether organization furnished equipment, contractor furnished equipment, or personal, that require any network access to a CMS network or system are securely configured and meet, as a minimum, the following security requirements: a. Up-to-date system patches; b. Current anti-virus software; c. Host-based intrusion detection system;

AC-17: Remote Access
d. Functionality that provides the capability for automatic execution of code disabled; and e. Employs required encryption (FIPS 140-2 validated module). 4. For organizations supporting remote access (including teleworking), ensure NIST SP 800-46 guidelines are followed by defining policies and procedures that define: a. Forms of permitted remote access; b. Types of devices permissible for remote access; c. Type of access remote users are granted; and d. How remote user account provisioning is handled.
Related Control Requirement(s): AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PL-4, SC-10, SI-4
Control Implementation Description: "Click here and type text" »

14.1.13.1 AC-17 (1): Automated Monitoring / Control

AC-17 (1): Automated Monitoring / Control
Control
The information system monitors and controls remote access methods. **Implementation Standard** The organization implements organization and industry best practice distributed blocking rules within one hour of receipt.
Related Control Requirement(s): AU-2, AU-12
Control Implementation Description: "Click here and type text"

14.1.13.2 AC-17 (2): Protection of Confidentiality / Integrity Using Encryption

AC-17 (2): Protection of Confidentiality / Integrity Using Encryption
Control
The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
Related Control Requirement(s): SC-8, SC-12, SC-13
Control Implementation Description: "Click here and type text"

14.1.13.3 AC-17 (3): Managed Access Control Points

AC-17 (3): Managed Access Control Points
Control
The information system routes all remote accesses through a limited number of managed access control points.
Related Control Requirement(s): SC-7
Control Implementation Description: "Click here and type text"

14.1.13.4 AC-17 (4): Privileged Commands / Access

AC-17 (4): Privileged Commands / Access
Control
The organization: a. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs; and b. Documents the rationale for such access in the security plan for the information system.
Related Control Requirement(s): AC-6
Control Implementation Description: "Click here and type text"

14.1.13.5 AC-17 (9): Disconnect / Disable Access

AC-17 (9): Disconnect / Disable Access
Control
The organization provides the capability to expeditiously disconnect or disable remote access to the information system within 15 minutes. **Implementation Standard** The organization terminates or suspends network connections (i.e., a system to system interconnection) upon issuance of an order by the CIO, CISO, or Senior Official for Privacy (SOP).
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.1.14 AC-18: Wireless Access

AC-18: Wireless Access
Control
The organization monitors for unauthorized wireless access to information systems and prohibits the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the organization CIO or a designated representative. If wireless access is authorized, the organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; b. Authorizes wireless access to the information system prior to allowing such connections; c. The organization ensures that: 1. The organization CIO must approve and distribute the overall wireless plan for his or her respective organization; and 2. Mobile and wireless devices, systems, and networks are not connected to wired organization networks except through appropriate controls (e.g., VPN port) or unless specific authorization from the organization network management has been received. **Implementation Standards** 1. If wireless access is explicitly authorized, wireless device service set identifier broadcasting is disabled and the following wireless restrictions and access controls are implemented: a. Encryption protection is enabled; b. Access points are placed in secure areas; c. Access points are shut down when not in use (i.e., nights, weekends); d. A firewall is implemented between the wireless network and the wired infrastructure; e. MAC address authentication is utilized; f. Static IP addresses, not Dynamic Host Configuration Protocol (DHCP), is utilized; g. Personal firewalls are utilized on all wireless clients; h. File sharing is disabled on all wireless clients; i. Intrusion detection agents are deployed on the wireless side of the firewall; j. Wireless activity is monitored and recorded, and the records are reviewed on a regular basis; k. Organizational policy related to wireless client access configuration and use is documented; 2. Wireless printers and all Bluetooth devices such as keyboards are not allowed without explicit approval by the organization's Authorizing Official (AO).
Related Control Requirement(s): AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4
Control Implementation Description: "Click here and type text"

14.1.14.1 AC-18 (1): Authentication and Encryption

AC-18 (1): Authentication and Encryption
Control
If wireless access is explicitly authorized, the information system protects wireless access to the system using encryption and authentication of both users and devices.

AC-18 (1): Authentication and Encryption
Related Control Requirement(s): SC-8, SC-13
Control Implementation Description: "Click here and type text"

14.1.15 AC-19: Access Control for Mobile Systems

AC-19: Access Control for Mobile Devices
Control
The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; b. Authorizes, through the organization CIO, the connection of mobile devices to organizational information systems **Implementation Standard** Encrypt information on all mobile devices that contains PII.
Related Control Requirement(s): AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-28, SI-3, SI-4
Control Implementation Description: "Click here and type text"

14.1.15.1 AC-19 (5): Full-Device / Container-Based Encryption

AC-19 (5): Full-Device / Container-Based Encryption
Control
The organization employs full-device encryption (FIPS 140-2 validated module), or container encryption, to protect the confidentiality and integrity of information on approved mobile devices. **Implementation Standard** Encrypt information on all mobile devices that contains PII.
Related Control Requirement(s): MP-5, SC-13, SC-28
Control Implementation Description: "Click here and type text"

14.1.16 AC-20: Use of External Information Systems

AC-20: Use of External Information Systems
Control
The organization prohibits the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process sensitive information, unless explicitly authorized, in writing, by the organization CIO or his/her designated representative. If external information systems are authorized, the organization establishes strict terms and conditions for their use. The terms and conditions must address, at a minimum: a. The types of applications that can be accessed from external information systems; b. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted; c. How other users of the external information system will be prevented from accessing federal information; d. The use of VPN and stateful inspection firewall technologies; e. The use of and protection against the vulnerabilities of wireless technologies; f. The maintenance of adequate physical security controls; g. The use of virus and spyware protection software; and h. How often the security capabilities of installed software are to be updated. **Implementation Standards** 1. Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Limit remote access only to information resources required by home users to complete job duties. Require that any organization-owned equipment be used only for business purposes by authorized employees. 2. Only organization owned computers and software can be used to process, access, and store PII. 3. Privacy requirements must be addressed in agreements that cover relationships in which external information systems are used to access, process, store, or transmit and manage PII. 4. Access to PII from external information systems (including, but not limited to, personally owned information systems/devices) is limited to those organizations and individuals with a binding agreement to terms and conditions of privacy requirements which protect the PII.
Related Control Requirement(s): AC-1, AC-3, AC-17, AC-19, CA-3, PL-4, SA-9
Control Implementation Description: "Click here and type text"

14.1.16.1 AC-20 (1): Limits on Authorized Use

AC-20 (1): Limits on Authorized Use
Control
The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: a. Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

AC-20 (1): Limits on Authorized Use
Related Control Requirement(s): CA-2
Control Implementation Description: "Click here and type text"

14.1.16.2 AC-20 (2): Portable Storage Devices

AC-20 (2): Portable Storage Devices
Control
The organization restricts the use of organization-controlled portable storage devices by authorized individuals on external information systems.
Related Control Requirement(s): AC-19 (5)
Control Implementation Description: "Click here and type text"

14.1.17 AC-21: Information Sharing

AC-21: Information Sharing
Control
The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for approved information-sharing circumstances where user discretion is required; and b. Employs defined automated mechanisms or manual processes (defined in the applicable security plan) to assist users in making information-sharing/collaboration decisions.
Related Control Requirement(s): AC-3
Control Implementation Description: "Click here and type text"

14.1.18 AC-22: Publicly Accessible Content

AC-22: Publicly Accessible Content
Control
The organization: a. Designates individuals authorized to post information onto a publicly accessible information system;

AC-22: Publicly Accessible Content
b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information at least quarterly and removes such information, if discovered. **Implementation Standard** The organization reviews the content on the publicly accessible organizational information system for nonpublic information at least quarterly
Related Control Requirement(s): AC-3, AC-4, AT-2, AT-3
Control Implementation Description: "Click here and type text"

14.2 Awareness and Training (AT)

14.2.1 AT-1: Security Awareness and Training Policy and Procedures

AT-1: Security Awareness and Training Policy and Procedures
Control
The organization: a. Develops, documents, and disseminates to personnel/roles as designated by the organization: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and, if necessary, updates the current: 1. Security awareness and training policy at least once every three (3) years; and 2. Security awareness and training procedures at least once every three (3) years.
Related Control Requirement(s): AR-5
Control Implementation Description: "Click here and type text"

14.2.2 AT-2: Security Awareness Training

AT-2: Security Awareness Training
Control
The organization provides basic security and privacy awareness training to information system users (including managers, senior executives, and contractors): b. As part of initial training for new users prior to accessing any system's information;

AT-2: Security Awareness Training
c. When required by system changes, and d. Within every three hundred sixty-five (365) days thereafter. **Implementation Standards** 1. An information security and privacy education and awareness training program is developed and implemented for all employees and contractors working on behalf of the organization and involved in accessing, using, managing or developing information systems. 2. Information security and privacy education awareness training must address individuals' responsibilities associated with sending sensitive information in email. 3. Security and privacy awareness training is provided before granting access to systems and networks, and within every three hundred sixty-five (365) days thereafter, to all employees and contractors to explain the importance and responsibility in safeguarding Personally Identifiable Information (PII) and ensuring privacy as established in federal legislation and OMB guidance.
Related Control Requirement(s): AT-3, AT-4, PL-4, AR-5
Control Implementation Description: "Click here and type text"

14.2.2.1 AT-2 (2): Insider Threat

AT-2 (2): Insider Threat
Control
The organization includes security and privacy awareness training on recognizing and reporting potential indicators of insider threats, such as: a. Inordinate, long-term job dissatisfaction, b. Attempts to gain access to information not required for job performance, c. Unexplained access to financial resources, d. Bullying or sexual harassment of fellow employees, e. Workplace violence, and f. Other serious violations of organizational policies, procedures, directives, rules or practices. **Implementation Standard** Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures.
Related Control Requirement(s): PL-4, PS-3, PS-6
Control Implementation Description: "Click here and type text"

14.2.3 AT-3: Role-Based Security Training

AT-3: Role-Based Security Training
Control
The organization provides role-based security and privacy training to personnel with assigned information security and privacy roles and responsibilities (i.e., significant information security and privacy responsibilities): a. Before authorizing access to the information system or performing assigned duties; and b. When required by information system changes; and c. Within sixty (60) days of entering a position that requires role-specific training, and every three hundred sixty-five (365) days thereafter. **Implementation Standards** 1. Require personnel with significant information security and privacy roles and responsibilities to undergo appropriate information system security and privacy training prior to authorizing access to networks, systems, and/or applications; when required by significant information system or system environment changes; when an employee enters a new position that requires additional role-specific training; and for refresher training within every three hundred sixty-five (365) days thereafter. 2. All personnel with significant information security roles and responsibilities that have not completed the required training within the mandated timeframes shall have their user accounts disabled until they have met their role-based training requirement
Related Control Requirement(s): AT-2, AT-4, PL-4, PS-7, SA-3, AR-5
Control Implementation Description: "Click here and type text"

14.2.4 AT-4: Security Training Records

AT-4: Security Training Records
Control
The organization: a. Identifies employees who hold roles with significant information security and privacy responsibilities; b. Documents and monitors individual information system security and privacy training activities, including basic security and privacy awareness training and specific role-based information system security and privacy training; and c. Retains individual training records for a minimum of five (5) years after the individual completes each training.
Related Control Requirement(s): AT-2, AT-3
Control Implementation Description: "Click here and type text"

14.3 Audit and Accountability (AU)

14.3.1 AU-1: Audit and Accountability Policy and Procedures

AU-1: Audit and Accountability Policy and Procedures
Control
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and updates (as necessary) the current: 1. Audit and accountability policy at least every 365 days; and 2. Audit and accountability procedures at least every 365 days.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.3.2 AU-2: Audit Events

AU-2: Audit Events
Control
The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system is capable of auditing the events specified in Implementation Standard 1; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; and c. Provides a rationale for why the auditable events are deemed to be adequate (relevant) to support after-the-fact investigations of security and privacy incidents; and d. Determines which events specified in Implementation Standard 2 require auditing on a continuous basis and which events require auditing in response to specific situations. **Implementation Standards** 1. List of auditable events: a. Server alerts and error messages; b. User log-on and log-off (successful or unsuccessful); c. All system administration activities; d. Modification of privileges and access; e. Start up and shut down; f. Application modifications; g. Application alerts and error messages; h. Configuration changes; i. Account creation, modification, or deletion; j. File creation and deletion; k. Read access to sensitive information; l. Modification to sensitive information; m. Printing sensitive information;

AU-2: Audit Events
n. Anomalous (e.g., non-attributable) activity; o. Data as required for privacy monitoring privacy controls; p. Concurrent log on from different work stations; q. Override of access control mechanisms; and r. Process creation. 2. Subset of Implementation Standard 1 auditable events: a. User log-on and log-off (successful or unsuccessful); b. Configuration changes; c. Application alerts and error messages; d. All system administration activities; e. Modification of privileges and access; f. Account creation, modification, or deletion; g. Concurrent log on from different work stations; and h. Override of access control mechanisms. 3. Verify that proper logging is enabled to audit administrator activities. 4. 5 U.S.C §552a(c) Accounting of Certain Disclosures: a. Each agency shall keep an accurate accounting of the date, nature and purpose of each disclosure of a record to any person/entity or other agency and the name and address of the person/entity or agency to whom the disclosure is made. The agency must retain the accounting for at least five years or the life of the record whichever is longer after the disclosure for which the accounting is made, make the accounting available to the individual named in the record at his request; and inform any person/entity or other agency about any correction or notation of dispute made by the agency of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.
Related Control Requirement(s): AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, SI-4, AR-8
Control Implementation Description: "Click here and type text"

14.3.2.1 AU-2 (3): Reviews and Updates

AU-2 (3): Reviews and Updates
Control
The organization reviews and updates the list of auditable events within every three hundred sixty-five (365) days or whenever there is change in the threat environment. **Implementation Standards** The System Owner reviews and approves the list of auditable events.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.3.3 AU-3: Content of Audit Records

AU-3: Content of Audit Records
Control
The information system generates audit records containing information that specifies: a. Date and time of the event; b. Component of the information system (e.g., software component, hardware component) where the event occurred; c. Type of event; d. User/subject identity; e. Outcome (success or failure) of the event; f. Execution of privileged functions; and g. Command line (for process creation events).
Related Control Requirement(s): AU-2, AU-8, AU-12, SI-11, AR-8
Control Implementation Description: "Click here and type text"

14.3.3.1 AU-3 (1): Additional Audit Information

AU-3 (1): Additional Audit Information
Control
The information system provides the capability to include more detailed information in the audit records for audit events that capture: a. Filename accessed; b. Program or command used to initiate the event; and c. Source and destination addresses. **Implementation Standards** 1. The information system includes: a. Additional, more detailed session, connection, transaction, or activity duration information; b. For client-server transactions, the number of bytes received and bytes sent; c. Additional informational messages to diagnose or identify the event; and d. Characteristics that describe or identify the object or resource acted upon in the audit records for audit events identified by type, location, or subject. 2. The organization defines audit record types. The audit record types are approved and accepted by the System Owner.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.3.4 AU-4: Audit Storage Capacity

AU-4: Audit Storage Capacity
Control
The organization allocates audit record storage capacity and configures auditing to reduce the likelihood that storage capacity will be exceeded. **Implementation Standard** Capacity must be sufficient to handle auditing records during peak performance times (e.g., open enrollment).
Related Control Requirement(s): AU-2, AU-5, AU-6, AU-7, AU-11, SI-4
Control Implementation Description: "Click here and type text"

14.3.5 AU-5: Response to Audit Processing Failures

AU-5: Response to Audit Processing Failures
Control
The information system: a. Alerts defined personnel or roles (defined in the applicable system security plan) in the event of an audit processing failure; and b. Takes the actions defined in Implementation Standard 1 in response to an audit failure or audit storage capacity issue. **Implementation Standards** 1. The information system takes the following action in response to an audit failure or audit storage capacity issue: a. Shutdown the information system or halt processing immediately; and b. Systems that do not support automatic shutdown must be shut down within 1 hour of the audit processing failure.
Related Control Requirement(s): AU-4, SI-12
Control Implementation Description: "Click here and type text"

14.3.5.1 AU-5 (1): Audit Storage Capacity

AU-5 (1): Audit Storage Capacity
Control
The information system provides a warning and alerts key personnel, roles, and/or locations (defined in the applicable security plan), within a defined time period (defined in the applicable security plan), when allocated audit record storage volume reaches 80 percent of the repository's maximum audit record storage capacity.
Related Control Requirement(s):

AU-5 (1): Audit Storage Capacity
Control Implementation Description:
«Click here and type text.]»

14.3.6 AU-6: Audit Review, Analysis, and Reporting

AU-6: Audit Review, Analysis, and Reporting
Control
The organization: a. Reviews and analyzes information system audit records no less often than weekly for indications of inappropriate or unusual activities defined within the Implementation Standards and reports findings to designated organizational officials (defined in the applicable security plan); and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in threat environment including operations, assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information. **Implementation Standards** 1. Review system records for initialization sequences, logons (successful and unsuccessful), errors, system processes, security software (e.g., malicious code protection, intrusion detection, firewall), applications, performance, and system resources utilization to determine anomalies no less than once within a twenty-four (24) hour period and on demand. Generate alert notification for technical personnel review and assessment. 2. Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies no less than once within a twenty-four (24) hour period and on demand. Generate alerts for technical personnel review and assessment. 3. Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action. 4. Use automated utilities to review audit records no less often than once every seventy-two (72) hours for unusual, unexpected, or suspicious behavior. 5. Inspect administrator groups on demand but no less often than once every fourteen (14) days to ensure unauthorized administrator, system, and privileged application accounts have not been created. 6. Perform manual reviews of system audit records randomly on demand but no less often than once every thirty (30) days.
Related Control Requirement(s):
AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, CA-7, CM-5, CM-8, CM-10, CM-11, IA-3, IA-5, IR-4, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7
Control Implementation Description:
"Click here and type text"

14.3.6.1 AU-6 (1): Process Integration

AU-6 (1): Process Integration
Control
The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. **Implementation Standards**

AU-6 (1): Process Integration
1. Aggregated audit records from automated information security capabilities and service tools must be searchable by the organization: a. Information is provided to the organization in a format compliant with Federal (e.g., Continuous Diagnostics and Mitigation) requirements; b. Audit records sources include systems, appliances, devices, services, and applications (including databases). c. Organization directed audit information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. 2. Raw audit records must be available in an unaltered format to the organization. 3. Raw security information/results from relevant automated tools must be available in an unaltered format to the organization.
Related Control Requirement(s): AU-12, PM-7
Control Implementation Description: "Click here and type text"

14.3.6.2 AU-6 (3): Correlate Audit Repositories

AU-6 (3): Correlate Audit Repositories
Control
The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. **Implementation Standards** 1. Correlated results from automated tools must be searchable by the organization: a. Repository sources include systems, appliances, devices, services, and applications (including databases); and b. Organization directed repository information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. 2. Raw audit records must be available in an unaltered format to the organization. 3. Raw security information/results from relevant automated tools must be available in an unaltered format to the organization.
Related Control Requirement(s): AU-12, IR-4
Control Implementation Description: "Click here and type text"

14.3.7 AU-7: Audit Reduction and Report Generation

AU-7: Audit Reduction and Report Generation
Control
The information system provides an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time marking of audit records.

AU-7: Audit Reduction and Report Generation
Related Control Requirement(s): AC-5, AU-6
Control Implementation Description: "Click here and type text"

14.3.7.1 AU-7 (1): Automatic Processing

AU-7 (1): Automatic Processing
Control
The information system provides the capability to process audit records for events of interest based on selectable event criteria.
Related Control Requirement(s): AU-2, AU-12
Control Implementation Description: "Click here and type text"

14.3.8 AU-8: Time Stamps

AU-8: Time Stamps
Control
The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and is accurate to within one hundred (100) milliseconds.
Related Control Requirement(s): AU-3, AU-12
Control Implementation Description: "Click here and type text"

14.3.8.1 AU-8 (1): Synchronization with Authoritative Time Source

AU-8 (1): Synchronization with Authoritative Time Source
Control
The information system synchronizes the internal clocks to the authoritative time source when the time difference is greater than thirty (30) seconds. **Implementation Standards**

AU-8 (1): Synchronization with Authoritative Time Source
1. The information system synchronizes internal information system clocks at least hourly with: http://tf.nist.gov/tf-cgi/servers.cgi 2. The organization selects primary and secondary time servers used by the National Institute of Standards and Technology (NIST) Internet time service. The secondary server is selected from a different geographic region than the primary server. 3. The organization synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.
Related Control Requirement(s): AU-12
Control Implementation Description: "Click here and type text"

14.3.9 AU-9: Protection of Audit Information

AU-9: Protection of Audit Information
Control
The information system protects audit information and audit tools from unauthorized access, modification, and deletion.
Related Control Requirement(s): AC-3, AC-6, MP-2, MP-4, PE-2, PE-3
Control Implementation Description: "Click here and type text"

14.3.9.1 AU-9 (4): Access by Subset of Privileged Users

AU-9 (4): Access by Subset of Privileged Users
Control
The organization authorizes access to management of audit functionality to only those individuals or roles who are not subject to audit by that system, and is defined in the applicable system security plan.
Related Control Requirement(s): AC-5
Control Implementation Description: "Click here and type text"

14.3.10 AU-10: Non-Repudiation

AU-10: Non-Repudiation
Control
The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed a particular action.
Related Control Requirement(s): SC-8, SC-12, SC-13, SC-17, SC-23
Control Implementation Description: "Click here and type text"

14.3.11 AU-11: Audit Record Retention

AU-11: Audit Record Retention
Control
The organization retains audit records online for at least ninety (90) days and archives old records off-line for ten (10) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. **Implementation Standards** 1. Audit inspection reports, including a record of corrective actions, are retained by the organization for a minimum of three (3) years from the date the inspection was completed. 2. When subject to a legal investigation (e.g., Insider Threat), audit records must be maintained until released by the investigating authority. 3. Audit record retention must comply with National Archives and Records Administration (NARA) or other authoritative mandate durations.
Related Control Requirement(s): AU-4, AU-5, AU-9, MP-6, DM-2
Control Implementation Description: "Click here and type text"

14.3.12 AU-12: Audit Generation

AU-12: Audit Generation
Control
The information system: a. Provides audit record generation capability for all auditable events defined in AU-2 and associated implementation standards including requirements of 5 U.S.C §552a(c), Accounting of Certain Disclosures and the following: 1. All successful and unsuccessful authorization attempts; 2. All changes to logical access control authorities (e.g., rights, permissions); 3. All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services; 4. The audit trail, which must capture the enabling or disabling of audit report generation services; and 5. The audit trail must capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database). b. Allows defined personnel or roles (defined in the applicable security plan) to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the list of events defined in AU-2 with the content defined in AU-3. **Implementation Standard** The information system provides audit record generation capability for the list of auditable events defined in AU-2 at all information system components where audit capability is deployed.
Related Control Requirement(s): AC-3, AU-2, AU-3, AU-6, AU-7, AR-8
Control Implementation Description: "Click here and type text"

14.4 Security Assessment and Authorization (CA)

14.4.1 CA-1: Security Assessment and Authorization Policy and Procedures

CA-1: Security Assessment and Authorization Policies and Procedures
Control
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and updates (as necessary) the current: 1. Security assessment and authorization policy at least every three (3) years; and 2. Security assessment and authorization procedures at least every three (3) years.

CA-1: Security Assessment and Authorization Policies and Procedures
Related Control Requirement(s): AR-1, AR-7
Control Implementation Description: "Click here and type text"

14.4.2 CA-2: Security Assessments

CA-2: Security Assessments
Control
The organization: a. Develops a security and privacy assessment plan that describes the scope of the assessment including: 1. Security and privacy controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security and privacy controls in the information system and its environment of operation every three hundred sixty-five (365) days to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces an assessment report that documents the results of the assessment; and d. Provides the results of the security and privacy control assessment within thirty (30) days after its completion, in writing, to the organizational official who is responsible for reviewing the assessment documentation and updating system security documentation where necessary to reflect any changes to the system. **Implementation Standards** 1. An independent assessment of all security and privacy controls must be conducted before the organization's Authorizing Official issues the authority to operate for all newly implemented, or significantly changed, systems. 2. Information system security assessments should be conducted annually. These assessments can be conducted by independent assessors or by the performance of self-assessments against the information system. 3. The annual security and privacy assessment requirement requires all security and privacy controls attributable to a system to be assessed.
Related Control Requirement(s): CA-5, CA-6, CA-7, RA-5, SA-11, SI-4
Control Implementation Description: "Click here and type text"

14.4.2.1 CA-2 (1): Independent Assessors

CA-2 (1): Independent Assessors
Control
The organization employs assessors or assessment teams with NIST-defined level of independence to conduct security and privacy control assessments of the organization's information system.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.4.3 CA-3: System Interconnections

CA-3: System Interconnections
Control
The organization: a. Authorizes connections from the organization's information system to other information systems through the use of interconnection security agreements (ISA); b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates the interconnection agreements on an ongoing basis to verify enforcement of security requirements; and; d. Establishes system-to-system connections with CMS through the CMS ISA process. e. Only activates a system interconnection (including testing) when a signed ISA is in place. **Implementation Standards** 1. Record each system interconnection in the security plan for the system that is connected to the remote location. 2. The ISA is updated following significant changes to the system, organization, or the nature of the electronic sharing of information that could impact the validity of the agreement. 3. The ISA must be fully signed and executed prior to any interconnection outside of the system boundary taking place for any purpose (within the constraints of the control).
Related Control Requirement(s): AC-3, AC-4, AC-20, AU-2, AU-12, CA-7, IA-3, SA-9, SC-7, SI-4
Control Implementation Description: "Click here and type text"

14.4.3.1 CA-3 (5): Restrictions on External System Connections

CA-3 (5): Restrictions on External System Connections
Control
The organization employs, and documents, in the applicable security plan a "deny all, permit-by-exception" policy for allowing defined information systems that receive, process, store, or transmit Personally Identifiable Information (PII) to connect to external information systems.

CA-3 (5): Restrictions on External System Connections
Related Control Requirement(s): CM-7
Control Implementation Description: "Click here and type text"

14.4.4 CA-5: Plan of Action and Milestones

CA-5: Plan of Action and Milestones
Control
The organization: a. Develops a plan of action and milestones (POA&M) for the information system within thirty (30) days of the final results for every internal/external audit/review or test (e.g., security controls assessment, penetration test) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; b. Updates the existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
Related Control Requirement(s): CA-2, CA-7, CM-4
Control Implementation Description: "Click here and type text"

14.4.5 CA-6: Security Authorization

CA-6: Security Authorization
Control
The organization: a. Ensures that the organizational authorizing official authorizes the information system for processing before commencing operations; and b. Updates the security authorization: 1. Within every three (3) years; 2. When significant changes are made to the system; 3. When changes in requirements result in the need to process data of a higher sensitivity; 4. When changes occur to authorizing legislation or federal requirements; 5. After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and 6. Prior to expiration of a previous security authorization. c. If the organization maintains a system-to-system connection with CMS through an executed ISA, the CMS-granted request to connect is updated: 1. Every year or three hundred sixty-five days; 2. When significant changes are made to the system; 3. When changes in requirements result in the need to process data of a higher sensitivity;

CA-6: Security Authorization
4. When changes occur to authorizing legislation or federal requirements; 5. After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and 6. Prior to expiration of a previous security authorization.
Related Control Requirement(s): CA-2, CA-7
Control Implementation Description: "Click here and type text"

14.4.6 CA-7: Continuous Monitoring

CA-7: Continuous Monitoring
Control
The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of organizationally defined metrics (defined in the applicable security plan) to be monitored annually and in accordance with the basic requirements set forth in the Non-Exchange Entity Information Security and Privacy Continuous Monitoring Strategy Guide consistent with the NIST SP 800-137, and b. Establishment of defined frequencies (defined in the applicable security plan) for monitoring and defined frequencies (defined in the applicable security plan) for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organizationally defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; g. Reporting the security status of organization and the information system to defined personnel or roles (defined in the applicable security plan) monthly; and h. Reporting the security status of organizational systems to defined personnel or roles (defined in the applicable security plan) at organizational-defined frequency, and reporting to CMS as specified in the implementation standard. **Implementation Standards** 1. When subject to a legal investigation (e.g., of an insider threat), continuous monitoring records must be maintained until released by the investigating authority. 2. Monitor systems, appliances, devices, and applications (including databases). 3. Identify specific review requirements for the following: a. Plan of Action and Milestones (POA&M) b. Reporting of significant changes to the organizational information system environment
Related Control Requirement(s): CA-2, CA-5, CA-6, CM-3, CM-4, RA-5, SA-11, SI-2, SI-4
Control Implementation Description: "Click here and type text"

14.4.6.1 CA-7 (1): Independent Assessment

CA-7 (1): Independent Assessment
Control
The organization employs assessors or assessment teams with a defined level of independence to monitor the security and privacy controls in the information system on an ongoing basis. **Implementation Standard** Implementation of independent security and privacy assessment and the Security Assessment Report (SAR) follows CMS specifications.
Related Control Requirement(s): CA-2
Control Implementation Description: "Click here and type text"

14.4.7 CA-8: Penetration Testing

CA-8: Penetration Testing
Control
The organization conducts both internal and external penetration testing, within every three hundred sixty-five (365) days, on defined information systems or system components (defined in the applicable system security plan), or whenever there has been a significant change to the system. At a minimum, penetration testing must be conducted to determine: a. How well the system tolerates real world-style attack patterns; b. The likely level of sophistication an attacker needs to successfully compromise the system; c. Additional countermeasures that could mitigate threats against the system; and d. Defenders' ability to detect attacks and respond appropriately. **Implementation Standards** 1. Conduct internal and external penetration testing as needed but no less often than once every three hundred sixty-five (365) days. 2. Penetration tests are performed when new risks and threats potentially affecting the system/applications are identified and reported or upon request from CMS. 3. Penetration testing on a production system must be conducted in a manner that minimized risk of information corruption or service outage.
Related Control Requirement(s): AP-1, AP-2, TR-1
Control Implementation Description: "Click here and type text"

14.4.7.1 CA-8 (1): Independent Penetration Agent or Team

CA-8 (1): Independent Penetration Agent or Team
Control
The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components. **Implementation Standard** The independent penetration agent or penetration team must be the organization CISO approved independent penetration test vendor.
Related Control Requirement(s): CA-2
Control Implementation Description: "Click here and type text"

14.4.8 CA-9: Internal System Connections

CA-9: Internal System Connections
Control
The organization: a. Authorizes connections of defined internal information system components or classes of components (defined in the applicable security plan) to the information system; and b. Documents, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated. Documentation must also address authorization and responsibilities of the receiving information system for protecting any PII. **Implementation Standard** The security plan will identify the types of personally owned equipment that may be internally connected with organizational information systems and networks.
Related Control Requirement(s): AC-3, AC-4, AC-18, AC-19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4
Control Implementation Description: "Click here and type text"

14.5 Configuration Management (CM)

14.5.1 CM-1: Configuration Management Policy and Procedures

CM-1: Configuration Management Policy and Procedures
Control
The organization: a. Develops, documents, and disseminates to applicable personnel:

CM-1: Configuration Management Policy and Procedures
1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and b. Reviews and updates (as necessary) the current: 1. Configuration management policy within every three (3) years; and 2. Configuration management procedures within every three (3) years. **Implementation Standard** The organization documents the configuration management process and procedures to: a. Define configuration items at the system and component level (e.g., hardware, software, and workstation); b. Monitor configurations; and c. Track and approve changes prior to implementation, including but not limited to, flaw remediation, security patches, and emergency changes (e.g., unscheduled changes such as mitigating newly discovered security vulnerabilities, system crashes, and replacement of critical hardware components).
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.5.2 CM-2: Baseline Configuration

CM-2: Baseline Configuration
Control
The organization develops, documents, and maintains under configuration control a current baseline configuration of the information system. **Implementation Standards** 1. Baseline configurations will be distilled from government, industry, and vendor standards and best practices. 2. Baseline configurations must include security updates. 3. Baseline configuration requirements apply to all systems, devices, appliances, and applications.
Related Control Requirement(s): CM-3, CM-6, CM-8, CM-9, SA-10
Control Implementation Description: "Click here and type text"

14.5.2.1 CM-2 (1): Reviews and Updates

CM-2 (1): Reviews and Updates
Control
The organization reviews and updates the baseline configuration of the information system: a. At least every three hundred sixty-five (365) days;

CM-2 (1): Reviews and Updates
b. When configuration settings change due to critical security patches, upgrades and emergency changes (e.g., unscheduled changes, system crashes, and replacement of critical hardware components), and major system changes/upgrades; c. As an integral part of information system component installations, upgrades, and updates to applicable governing standards (implemented within the 365 days specified in number 1 above); and d. Supporting baseline configuration documentation reflects ongoing implementation of operational configuration baseline updates, either directly or by policy. **Implementation Standard** The organization reviews and updates the baseline configuration of the information system: a. Annually; b. When required due to a significant change; and c. As an integral part of information system component installations and upgrades.
Related Control Requirement(s): CM-5
Control Implementation Description: "Click here and type text"

14.5.2.2 CM-2 (3): Retention of Previous Configurations

CM-2 (3): Retention of Previous Configurations
Control
The organization retains older versions of baseline configurations of the information system as deemed necessary to support rollback. **Implementation Standard** Following baseline configuration updates, no less than one (1) older baseline configuration must be maintained (e.g., for emergency rollback).
Related Control Requirement(s):
Control Implementation Description:
"Click here and type text"

14.5.3 CM-3: Configuration Change Control

CM-3: Configuration Change Control
Control
The organization: a. Determines the types of changes to the information system that are configuration-controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system;

CM-3: Configuration Change Control
e. Retains records of configuration-controlled changes to the information system for a minimum of three (3) years after the change; f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through change request forms that must be approved by an organizational change control board that convenes frequently enough to accommodate proposed change requests, and by other appropriate organization officials including, but not limited to, the System Developer/Maintainer and information system support staff. **Implementation Standards** 1. The organization coordinates and provides oversight for configuration change control activities through organization-defined configuration change control element (e.g., committee or board) that convenes at an organization-defined frequency and according to organization-defined configuration change conditions. 2. The organization defines the configuration change control element and the frequency or conditions under which it is convened. 3. The organization establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its business agreements/contracts with CMS and business partners, and services to the business owner and associated service consumers (e.g., electronic bulletin board, or web status page). The means of communication are approved and accepted by the organization.
Related Control Requirement(s): CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12
Control Implementation Description: "Click here and type text"

14.5.3.1 CM-3 (2): Test / Validate / Document Changes

CM-3 (2): Test / Validate / Document Changes
Control
The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.5.4 CM-4: Security Impact Analysis

CM-4: Security Impact Analysis
Control
The organization analyzes changes to the information system to determine potential security and privacy impacts prior to change implementation. Activities associated with configuration changes to the information system are audited.

CM-4: Security Impact Analysis
Implementation Standard A security and privacy impact analysis is recommended as part of change management.
Related Control Requirement(s): CA-2, CA-7, CM-3, CM-9, SA-5, SA-10, SI-2
Control Implementation Description: "Click here and type text"

14.5.4.1 CM-4 (1): Separate Test Environments

CM-4 (1): Separate Test Environments
Control
The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.
Related Control Requirement(s): AP-2, DM-2, DM-3, SA-11, SC-7, UL-1
Control Implementation Description: "Click here and type text"

14.5.5 CM-5: Access Restrictions for Change

CM-5: Access Restrictions for Change
Control
The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes shall be generated, reviewed, and retained.
Related Control Requirement(s): AC-3, AC-5, AC-6, PE-3
Control Implementation Description: "Click here and type text"

14.5.5.1 CM-5 (1): Automated Access Enforcement / Auditing

CM-5 (1): Automated Access Enforcement / Auditing
Control
The organization employs automated mechanisms to enforce access restrictions to configuration change information and support auditing of the enforcement actions.

CM-5 (1): Automated Access Enforcement / Auditing
Related Control Requirement(s): AU-2, AU-6, AU-12, CM-3, CM-6
Control Implementation Description: "Click here and type text"

14.5.5.2 CM-5 (5): Limit Production / Operational Privileges

CM-5 (5): Limit Production / Operational Privileges
Control
The organization: a. Limits privileges to change information system components and system-related information within a production or operational environment; and b. Reviews and reevaluates privileges at least quarterly.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.5.6 CM-6: Configuration Settings

CM-6: Configuration Settings
Control
The organization: a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using the latest security configuration guidelines listed in Implementation Standard 1 that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for individual components within the information system based on explicit operational requirements (defined in the applicable system security plan); and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. **Implementation Standards** 1. Security configuration guidelines may be developed by different federal agencies. Therefore, it is possible that a guideline could include configuration information that conflicts with another agency or the organization's guideline. To resolve configuration conflicts among multiple security guidelines, the organization's hierarchy for implementing all security configuration guidelines is as follows: a. NIST; b. CMS; c. Defense Information Systems Agency (DISA), Security Technical Implementation Guides (STIG);

CM-6: Configuration Settings
d. Office of Management and Budget (OMB); e. U.S. Government Configuration Baselines (USGCB), 2. The organization must use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establish own configuration settings if USGCB is not available. 3. The organization ensures that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available).
Related Control Requirement(s): AC-19, CM-2, CM-3, CM-7, CM-8, SI-4
Control Implementation Description: "Click here and type text"

14.5.6.1 CM-6 (1): Automated Central Management / Application / Verification

CM-6 (1): Automated Central Management / Application / Verification
Control
The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for information technology products.
Related Control Requirement(s): CA-7, CM-4
Control Implementation Description: "Click here and type text"

14.5.7 CM-7: Least Functionality

CM-7: Least Functionality
Control
The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of high-risk system services, ports, network protocols, and capabilities (e.g., Telnet, FTP, etc.) across network boundaries that are not explicitly required for system or application functionality. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the applicable security plan; all others will be disabled. c. A list of specifically needed system services, ports, and network protocols must be maintained and documented in the applicable security plan; all others will be disabled. **Implementation Standards** 1. The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: United States Government Configuration Baseline (USGCB)-defined list of prohibited or restricted functions, ports, protocols, and/or services. 2. The organization shall use the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available.

CM-7: Least Functionality
Related Control Requirement(s): AC-6, CM-2, RA-5, SA-5, SC-7
Control Implementation Description: "Click here and type text"

14.5.7.1 CM-7 (1): Periodic Review

CM-7 (1): Periodic Review
Control
The organization: a. Reviews the information system at least quarterly to identify and eliminate unnecessary functions, ports, protocols, and/or services; b. Performs periodic review at least quarterly of the information system to identify changes in functions, ports, protocols, and/or services; and c. Disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.
Related Control Requirement(s): AC-18, CM-7, IA-2
Control Implementation Description: "Click here and type text"

14.5.7.2 CM-7 (2): Prevent Program Execution

CM-7 (2): Prevent Program Execution
Control
The information system prevents program execution in accordance with policies regarding authorized software use which include, but are not limited to the following: a. Software must be legally licensed; b. Software must be provisioned in approved configurations; and c. Users must be authorized for software program use.
Related Control Requirement(s): CM-8
Control Implementation Description: "Click here and type text"

14.5.7.3 CM-7 (4): Unauthorized Software / Blacklisting

CM-7 (4): Unauthorized Software / Blacklisting
Control
The organization: a. Identifies defined software programs (defined in the applicable security plan) not authorized to execute on the information system; b. Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; c. Reviews and updates the list of unauthorized software programs quarterly; and d. Receives automated updates from a trusted source.
Related Control Requirement(s): CM-6, CM-8
Control Implementation Description: "Click here and type text"

14.5.8 CM-8: Information System Component Inventory

CM-8: Information System Component Inventory
Control
The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes: a. Each component's unique identifier and/or serial number; b. Information system of which the component is a part; c. Type of information system component (e.g., server, desktop, application); d. Manufacturer/model information; e. Operating system type and version/service pack level; f. Presence of virtual machines; g. Application software version/license information; h. Physical location (e.g., building/room number); i. Logical location (e.g., IP address, position with the information system [IS] architecture); j. Media access control (MAC) address; k. Ownership; l. Operational status; m. Primary and secondary administrators; and n. Primary user. b. Reviews and updates the information system component inventory no less than every three hundred sixty-five (365) days, or per CM-8 (1) and/or CM-8 (2), as applicable. **Implementation Standards** 1. The organization defines information deemed necessary to achieve effective property accountability. 2. The organization establishes, maintains, and updates, within every three hundred sixty-five (365) days, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII).

CM-8: Information System Component Inventory
3. Fully integrate inventory of information system components with the organizational continuous monitoring capability. 4. Automated asset inventory information tracking systems must: a. Transmit updates to organization based upon organizational defined frequency; 5. Automated component tracking and management tool results must be searchable by the organization: a. Information is provided to the organization in a format compliant with organizational defined continuous monitoring requirements; b. Authorized component information sources include systems, platforms, appliances, devices; c. Component information sources that do not support the exchange of information with the organization must be documented in the applicable risk assessment and security plan; and d. Organization directed authorized component information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. 6. Raw security information/results from relevant automated tools must be available in an unaltered format to the organization.
Related Control Requirement(s): CM-2, CM-6, SE-1
Control Implementation Description: "Click here and type text"

14.5.8.1 CM-8 (1): Updates During Installations / Removals

CM-8 (1): Updates During Installations / Removals
Control
The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.5.8.2 CM-8 (3): Automated Unauthorized Component Detection

CM-8 (3): Automated Unauthorized Component Detection
Control
The organization: a. Employs automated mechanisms to scan the network no less than weekly to detect the presence of unauthorized hardware, software, and firmware components within the information system; and b. Takes the following actions when unauthorized components are detected: 1. Disable access to the identified component; 2. Disables network access by such components/devices; 3. Isolates the identified component; and

CM-8 (3): Automated Unauthorized Component Detection
4. Notifies defined personnel or roles (defined in the applicable security plan). **Implementation Standards** In a shared computing facility, the organization: 1. Employs automated mechanisms to scan continuously, using automated mechanisms with a maximum (5) five-minute delay in detection to detect the addition of unauthorized components/devices into the information system; and 2. Disables network access by such components/devices or notifies designated organizational officials.
Related Control Requirement(s): AC-17, AC-18, AC-19, CA-7, CM-8, RA-5, SI-3, SI-4, SI-7
Control Implementation Description: "Click here and type text"

14.5.8.3 CM-8 (5): No Duplicate Accounting of Components

CM-8 (5): No Duplicate Accounting of Components
Control
The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.5.9 CM-9: Configuration Management Plan

CM-9: Configuration Management Plan
Control
The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying and managing configuration items throughout the system development life cycle; c. Defines the configuration items for the information system; d. Places the configuration items under configuration management; and e. Protects the configuration management plan from unauthorized disclosure and modification. f. Reviews and updates (as necessary) the current configuration management plan within every year.

CM-9: Configuration Management Plan
Related Control Requirement(s): CM-2, CM-3, CM-4, CM-5, CM-8, SA-10
Control Implementation Description: The Configuration Management Plan is a required artifact**.** "Click here and type text"

14.5.10 CM-10: Software Usage Restrictions

CM-10: Software Usage Restrictions
Control
The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
Related Control Requirement(s): AC-17, CM-8, SC-7
Control Implementation Description: "Click here and type text"

14.5.10.1 CM-10 (1): Open Source Software

CM-10 (1): Open Source Software
Control
The organization establishes restrictions on the use of open source software. Open source software must: a. Be legally licensed; b. Approved by the agency information technology department; and c. Adhere to a secure configuration baseline checklist from the U.S. Government or industry.
Related Control Requirement(s): AC-17, CM-8, SC-7
Control Implementation Description: "Click here and type text"

14.5.11 CM-11: User-Installed Software

CM-11: User-Installed Software
Control
The organization: a. Establishes organization-defined policies governing the installation of software by users; b. Enforces software installation policies through organization-defined methods; and c. Monitors policy compliance organization-defined frequency. **Implementation Standard** Monitoring for user-installed software must comply with organizational defined continuous monitoring requirements.
Related Control Requirement(s): AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4
Control Implementation Description: "Click here and type text"

14.6 Contingency Planning (CP)

14.6.1 CP-1: Contingency Planning Policy and Procedures

CP-1: Contingency Planning Policy and Procedures
Control
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. b. Reviews and updates (as necessary) the current: 1. Contingency planning policy at least every three (3) years or as necessitated by significant change. 2. Contingency planning procedures at least every three (3) years or as necessitated by significant change.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.6.2 CP-2: Contingency Plan

CP-2: Contingency Plan
Control
The organization: a. Develops a contingency plan for the information system in accordance with NIST SP 800-34 that:

CP-2: Contingency Plan
1. Identifies essential organizational missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential organizational missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by designated officials within the organization; b. Distributes copies of the contingency plan to the Information System Security Officer, Business Owner, Contingency Plan Coordinator, and other stakeholders identified within the contingency plan; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system within every three hundred sixty-five (365) days; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to key contingency personnel system administrator, database administrator, and other personnel/roles as appropriate and organizational elements identified above; and g. Protects the contingency plan from unauthorized disclosure and modification. **Implementation Standards** 1. The system must be continuously monitored and assessed to ensure that it is operating as intended and that changes do not have an adverse effect on system performance. 2. The organization must verify that the provisioned implementation being assessed and/or monitored meets users' needs and is an approved system configuration. 3. The organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements to whom the organization will distribute the CP. 4. The organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements to whom the organization will communicate any CP changes.
Related Control Requirement(s): AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5
Control Implementation Description: The Contingency Plan is a required artifact. "Click here and type text"

14.6.2.1 CP-2 (1): Coordinate with Related Plans

CP-2 (1): Coordinate with Related Plans
Control
The organization coordinates contingency plan development with organizational elements responsible for related plans.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.6.2.2 CP-2 (2): Capacity Planning

CP-2 (2): Capacity Planning
Control
The organization conducts capacity planning to ensure the necessary capacity for information processing, telecommunications, and environmental support during contingency operations.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.6.2.3 CP-2 (3): Resume Essential Missions / Business Functions

CP-2 (3): Resume Essential Missions / Business Functions
Control
The organization plans for the resumption of essential missions and business functions within the approved Maximum Tolerable Downtime (MTD), determined by the business owner, for the business functions.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.6.2.4 CP-2 (8): Identity Critical Assets

CP-2 (8): Identify Critical Assets
Control
The organization identifies critical information system assets supporting essential missions and business functions.
Related Control Requirement(s): SA-15
Control Implementation Description: "Click here and type text"
Assessment Procedure:

14.6.3 CP-3: Contingency Training

CP-3: Contingency Training
Control
The organization provides contingency training to operational and support personnel (including managers and information system users) consistent with assigned roles and responsibilities:

CP-3: Contingency Training
a. Within ninety (90) days of assuming a contingency role or responsibility; b. When required by information system changes; and c. Within every three hundred sixty-five (365) days thereafter.
Related Control Requirement(s): AT-2, AT-3, CP-2, IR-2
Control Implementation Description: "Click here and type text"

14.6.4 CP-4: Contingency Plan Testing

CP-4: Contingency Plan Testing
Control
The organization: a. Tests the contingency plan for the information system within every three hundred sixty-five (365) days using NIST or organization-defined tests and exercises, such as tabletop tests, in accordance with the current organization contingency plan procedure to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the contingency plan test results; and c. Initiates corrective actions, if needed. **Implementation Standards** 1. Must produce an after-action report to improve existing processes, procedures, and policies. 2. Contingency plan test results will be made available to the organization business owner and all system developers and maintainers.
Related Control Requirement(s): CP-2, CP-3, IR-3
Control Implementation Description: The Contingency Plan Test Results is a required artifact. "Click here and type text"

14.6.4.1 CP-4 (1): Coordinate with Related Plans

CP-4 (1): Coordinate with Related Plans
Control
The organization coordinates contingency plan testing with organizational elements responsible for related plans. **Implementation Standards** Organizations require a suite of plans to prepare themselves for response, continuity, recovery, and resumption of mission/business processes and information systems in the event of a disruption. Each plan has a specific purpose and scope: 1. Continuity of Operations Plan (COOP) 2. Business Continuity Plan (BCP) 3. Critical Infrastructure Protection (CIP) Plan

CP-4 (1): Coordinate with Related Plans
4. Disaster Recovery Plan (DRP) 5. Information System Contingency Plan (ISCP) 6. Cyber Incident Response Plan 7. Occupant Emergency Plan (OEP)
Related Control Requirement(s): IR-8
Control Implementation Description: "Click here and type text"

14.6.5 CP-6: Alternate Storage Site

CP-6: Alternate Storage Site
Control
The organization: a. Establishes an alternate storage site as well as the necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.
Related Control Requirement(s): CP-2, CP-9, CP-10, MP-4
Control Implementation Description: "Click here and type text"

14.6.5.1 CP-6 (1): Separation from Primary Site

CP-6 (1): Separation from Primary Site
Control
The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.
Related Control Requirement(s): RA-3
Control Implementation Description: "Click here and type text"

14.6.5.2 CP-6 (3): Accessibility

CP-6 (3): Accessibility
Control
The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.
Related Control Requirement(s): RA-3
Control Implementation Description: "Click here and type text"

14.6.6 CP-8: Telecommunications Services

CP-8: Telecommunications Services
Control
The organization establishes alternate telecommunications services including the necessary agreements to permit the resumption of information system operations for essential organizational missions and business functions within the resumption time period specified in Implementation Standard 1 when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. **Implementation Standards** 1. Ensure alternate telecommunications service level agreements (SLAs) are in place to permit resumption of system Recovery Time Objectives (RTO) and business functions Maximum Tolerable Downtimes (MTD). 2. The system owner defines a resumption time period consistent with the RTOs and business impact analysis. The time period is approved and accepted by the business owner.
Related Control Requirement(s): CP-2, CP-6
Control Implementation Description: "Click here and type text"

14.6.6.1 CP-8 (1): Priority of Service Provisions

CP-8 (1): Priority of Service Provisions
Control
The organization: a. Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and b. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.
Related Control Requirement(s):

CP-8 (1): Priority of Service Provisions
Control Implementation Description:
"Click here and type text"

14.6.6.2 CP-8 (2): Single Points of Failure

CP-8 (2): Single Points of Failure
Control
The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.
Related Control Requirement(s):
Control Implementation Description:
"Click here and type text"

14.6.7 CP-9: Information System Backup

CP-9: Information System Backup
Control
The organization: a. Conducts backups of user-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1; b. Conducts backups of system-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1; c. Conducts backups of information system documentation, including security-related documentation, other forms of data, and paper records, within the frequency defined in the applicable security plan, consistent with recovery time and recovery point objectives; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations. **Implementation Standards** 1. Perform full backups weekly to separate media. Perform incremental or differential backups daily to separate media. Backups to include user-level and system-level information (including system state information). Three (3) generations of backups (full as well as all related incremental or differential backups) are stored off site. Off-site and on-site backups must be logged with name, date, time and action. 2. The organization determines how Information System Backup is going to be verified and the appropriate periodicity of the check. 3. Backups must be compliant with requirements for protecting data at rest. (see SC-28). 4. The organization maintains at least three (3) backup copies of user-level information, system-level information, and information system documentation including security information (at least one (1) of which is available online) or provides an equivalent alternative. 5. Ensure that a current, retrievable, copy of Personally Identifiable Information (PII) is available before movement of servers. 6. (Cloud environments) The system owner shall determine what elements of the cloud environment require the Information System Backup control.

CP-9: Information System Backup
7. (Cloud environments) The system owner determines how Information System Backup will be verified and the appropriate periodicity of the check. 8. Use the encryption methodology specified in SC-13 to encrypt personally identifiable information (PII) confidentiality impact level information in backups at the storage location.
Related Control Requirement(s): CP-2, CP-6, MP-4, MP-5, SC-13
Control Implementation Description: "Click here and type text"

14.6.7.1 CP-9 (1): Testing for Reliability / Integrity

CP-9 (1): Testing for Reliability / Integrity
Control
The organization tests backup information following each backup, at least every six months to verify media reliability and information integrity.
Related Control Requirement(s): CP-4
Control Implementation Description: "Click here and type text"

14.6.8 CP-10: Information System Recovery and Reconstitution

CP-10: Information System Recovery and Reconstitution
Control
The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner. **Implementation Standard** Secure information system recovery and reconstitution includes, but is not limited to: a. Reset all system parameters (either default or organization-established); b. Reinstall patches; c. Reestablish configuration settings; d. Reinstall application and system software; and e. Fully test the system.
Related Control Requirement(s): CA-2, CA-6, CA-7, CP-2, CP-6, CP-9
Control Implementation Description: "Click here and type text"

14.6.8.1 CP-10 (2): Transaction Recovery

CP-10 (2): Transaction Recovery
Control
The information system implements transaction recovery for transaction-based systems.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.7 Identification and Authentication (IA)

14.7.1 IA-1: Identification and Authentication Policy and Procedures

IA-1: Identification and Authentication Policy and Procedures
Control
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. b. Reviews and updates (as necessary) the current: 1. Identification and authentication policy at least every three (3) years; and 2. Identification and authentication procedures at least every three (3) years.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.7.2 IA-2: User Identification and Authentication (Organizational Users)

IA-2: Identification and Authentication (Organizational Users)
Control
The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). **Implementation Standards** 1. Require the use of system and/or network authenticators and unique user identifiers. 2. Help desk support requires user identification for any transaction that has information security implications.

IA-2: Identification and Authentication (Organizational Users)
Related Control Requirement(s): AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8
Control Implementation Description: "Click here and type text"

14.7.2.1 IA-2 (1): Network Access to Privileged Accounts

IA-2 (1): Network Access to Privileged Accounts
Control
The information system implements multifactor authentication for network access to privileged accounts.
Related Control Requirement(s): AC-6
Control Implementation Description: "Click here and type text"

14.7.2.2 IA-2 (2): Network Access to Non-Privileged Accounts

IA-2 (2): Network Access to Non-Privileged Accounts
Control
The information system implements multifactor authentication for network access to non-privileged accounts.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.7.2.3 IA-2 (3): Local Access to Privileged Accounts

IA-2 (3): Local Access to Privileged Accounts
Control
The information system implements multifactor authentication for local access to privileged accounts.
Related Control Requirement(s): AC-6
Control Implementation Description: "Click here and type text"

14.7.2.4 IA-2 (8): Network Access to Privileged Accounts – Replay Resistant

IA-2 (8): Network Access to Privileged Accounts – Replay Resistant
Control
The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.7.2.5 IA-2 (11): Remote Access – Separate Device

IA-2 (11): Remote Access – Separate Device
Control
The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.
Related Control Requirement(s): AC-6
Control Implementation Description: "Click here and type text"

14.7.3 IA-3: Device Identification and Authentication

IA-3: Device Identification and Authentication
Control
The information system uniquely identifies and authenticates defined types of devices (defined in the applicable security plan) that require authentication mechanisms which, at a minimum, use shared information [Media Access Control (MAC) or Internet Protocol (IP) address] and access control lists to control remote network access prior to establishing the connection. If remote authentication is provided by the system itself, the system must follow most recent NIST SP 800-63 Digital Identify Guidelines. **Implementation Standard** The organization defines a list a specific devices and/or types of devices approved and accepted for identification and authentication management.
Related Control Requirement(s): AC-17, AC-18, AC-19, CA-3, IA-4, IA-5
Control Implementation Description: "Click here and type text"

14.7.4 IA-4: Identifier Management

IA-4: Identifier Management
Control
The organization manages information system identifiers by: a. Receiving authorization from defined personnel or roles (defined in the applicable security plan) to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of three (3) years or more has passed; and e. Disabling the identifier after sixty (60) days or less of inactivity and deleting disabled accounts during the annual re-certification process. **Implementation Standards** 1. The organization defines time period of inactivity for device identifiers. 2. Social security numbers (SSNs), and parts of SSNs, must not be used as system identifiers. Identifier management must ensure that any access to, or action involving, personally identifiable information (PII) is attributable to a unique individual.
Related Control Requirement(s): AC-2, IA-2, IA-3, IA-5, IA-8
Control Implementation Description: "Click here and type text"

14.7.5 IA-5: Authenticator Management

IA-5: Authenticator Management
Control
The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators as follows: 1. Passwords are valid for no longer than the period directed in IA-5 (1) immediately in the event of known or suspected compromise, and immediately upon system installation (e.g. default or vendor-supplied passwords); 2. Public Key Infrastructure (PKI) certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three (3) years; and 3. Any PKI authentication request must be validated by Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) to ensure that the certificate being used for authentication has not been revoked.

IA-5: Authenticator Management
4. All other authenticator types every sixty (60) days; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts change.
Related Control Requirement(s): AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28
Control Implementation Description: "Click here and type text"

14.7.5.1 IA-5 (1): Password-Based Authentication

IA-5 (1): Password-Based Authentication
Control
For password-based authentication, the information systems follow the direction in the applicable configuration baselines per CM-6, or as follows, whichever is more stringent: a. Allows the use of a temporary password for system logons with an immediate change to a permanent password. b. Password Complexity: User Accounts: Enforces minimum password complexity of case sensitive, minimum of eight (8) characters, and at least one (1) each of upper-case letters, lower-case letters, numbers, and special characters; c. Prohibits the use of dictionary names or words; d. Enforces at least the following minimum password requirements for Users / Privileged Users / Processes [acting on behalf of a User]: 1. MinimumPasswordAge = 1/1/1; 2. MaximumPasswordAge = 60/60/60 3. MinimumPasswordLength = 8/15/15 e. Enforces at least six (6) changed characters or as determined by the information system (where possible) when new passwords are created; f. Encrypts passwords in storage and in transmission; g. Prohibit password reuse for 24 generations; and h. Password-protect system initialization (boot) settings. **Implementation Standard** Mobile devices are excluded from the password complexity requirement.
Related Control Requirement(s): IA-6
Control Implementation Description: "Click here and type text"

14.7.5.2 IA-5 (2): PKI-Based Authentication

IA-5 (2): PKI-Based Authentication
Control
For PKI-based authentication, the information system: a. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; b. Enforces authorized access to the corresponding private key; c. Maps the authenticated identity to the account of the individual or group; and d. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.
Related Control Requirement(s): IA-6
Control Implementation Description: "Click here and type text"

14.7.5.3 IA-5 (3): In-Person or Trusted Third-Party Registration

IA-5 (3): In-Person or Trusted Third-Party Registration
Control
The organization requires that the registration process to receive hardware administrative tokens and credentials used for two (2)-factor authentication be conducted in person before a designated registration authority with authorization by defined personnel or roles (defined in the applicable security plan).
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.7.5.4 IA-5 (7) No Embedded Unencrypted Static Authenticators

IA-5 (7): No Embedded Unencrypted Static Authenticators
Control
The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.7.5.5 IA-5 (11): Hardware Token-Based Authentication

IA-5 (11): Hardware Token-Based Authentication
Control
The information system, for hardware token-based authentication, employs mechanisms that satisfy minimum token requirements as defined by the organization.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.7.6 IA-6: Authenticator Feedback

IA-6: Authenticator Feedback
Control
The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
Related Control Requirement(s): PE-18
Control Implementation Description: "Click here and type text"

14.7.7 IA-7: Cryptographic Module Authentication

IA-7: Cryptographic Module Authentication
Control
The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.
Related Control Requirement(s): SC-12, SC-13
Control Implementation Description: "Click here and type text"

14.7.8 IA-8: Identification and Authentication (Non-Organizational Users)

IA-8: Identification and Authentication (Non-Organizational Users)
Control
The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users prior to gaining access to all organizational systems and networks (unless a risk-based decision is made for a system that does not require non-organization user authentication).
Related Control Requirement(s): AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3
Control Implementation Description: "Click here and type text"

14.7.8.1 IA-8 (2): Authentication of Third-Party Credentials

IA-8(2): Acceptance of Third-Party Credentials
Control
The information system accepts only FICAM approved third-party credentials.
Related Control Requirement(s): AU-2
Control Implementation Description: "Click here and type text"

14.8 Incident Response (IR)

14.8.1 IR-1: Incident Response Policy and Procedures

IR-1: Incident Response Policy and Procedures
Control
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls that are consistent with CMS Incident and Breach Notification Procedures within the CMS Risk Management Handbook. b. Reviews and updates (as necessary) the current: 1. Incident response policy within every three (3) years; and 2. Incident response procedures within every three (3) years.

IR-1: Incident Response Policy and Procedures
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.8.2 IR-2: Incident Response Training

IR-2: Incident Response Training
Control
The organization provides incident response training consistent with assigned roles and responsibilities to information system users: a. Within one (1) month of assuming an incident response role or responsibility; b. When required by information system changes; and c. Within every three hundred sixty-five (365) days thereafter. **Implementation Standard** Formally tracks personnel participating in incident response training.
Related Control Requirement(s): AT-3, CP-3, IR-8, AR-5
Control Implementation Description: "Click here and type text"

14.8.3 IR-3: Incident Response Testing

IR-3: Incident Response Testing
Control
The organization tests the incident response capability for the information system, reviews and analyzes the results, performs simulations, and documents the test results to determine the incident response effectiveness within every three hundred sixty-five (365) days using NIST SP 800-61. **Implementation Standards** 1. Incident response capability tests must exercise (or simulate exercise of) all organizational response capabilities. The organization's documented response to an actual historic incident may be used as part of an incident response capability test, and any response capabilities that were not exercised as part of the previous actual incident response activities must be additionally exercised (or simulated) as part of the test. 2. The organization defines tests and/or exercises in accordance with NIST SP 800-61 (as amended).
Related Control Requirement(s): CP-4, IR-8
Control Implementation Description: "Click here and type text"

14.8.3.1 IR-3 (2): Coordination with Related Plans

IR-3 (2): Coordination with Related Plans
Control
The organization coordinates incident response testing with organizational elements responsible for related plans.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.8.4 IR-4: Incident Handling

IR-4: Incident Handling
Control
The organization: a. Implements an incident handling capability (i.e., system incident response plan) using the current NIST SP 800-61; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises and implements the resulting changes accordingly. d. Ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system. **Implementation Standards** 1. Document relevant information related to a security incident per the current organization incident handling and breach notification procedures. 2. Preserve evidence through technical means, including secured storage of evidence media and “write” protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow a chain of custody for forensic evidence. 3. Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure, including isolating or disconnecting systems. 4. Incident response activities, to include forensic malware analysis, is coordinated with the ISSO. Each organization’s security operations center: a. Is responsible for actions to reduce the risk that an information security and/or privacy incident will occur and to respond appropriately to each incident or breach; and b. Maintains primary responsibility for incident detection, including internal security monitoring and analysis of network traffic and logs. 5. Contact information for individuals with incident handling responsibilities must be maintained in the system Incident Response Plan. a. Changes must be documented in the system incident response plan within three (3) days of the change.

IR-4: Incident Handling
Related Control Requirement(s): AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, SC-5, SC-7, SI-3, SI-4, SI-7
Control Implementation Description: "Click here and type text"

14.8.4.1 IR-4 (1): Automated Incident Handling Processes

IR-4 (1): Automated Incident Handling Processes
Control
The organization employs automated mechanisms to support the incident handling process. **Implementation Standards** 1. Automated mechanisms support the exchange of incident handling information within the organization: a. Information is provided in a format compliant with incident handling procedure; b. Incident handling information sources include systems, appliances, devices, services, and applications (including databases). c. Incident handling information sources that do not support the exchange of information must be documented in the applicable risk assessment and security plan; and d. Organization directed incident handling information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. 2. Raw audit records must be available in an unaltered format.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.8.5 IR-5: Incident Monitoring

IR-5: Incident Monitoring
Control
The organization tracks and documents all physical, information security, and privacy incidents. **Implementation Standards** 1. The organization forwards information system security and privacy incident and breach information: In accordance with reporting requirements defined in applicable incident response plans; and 2. Provides incident and breach information in format compliant with organizational defined continuous monitoring requirements.
Related Control Requirement(s): AU-6, IR-8, SC-5, SC-7, SI-3, SI-4, SI-7
Control Implementation Description: "Click here and type text"

14.8.6 IR-6: Incident Reporting

IR-6: Incident Reporting
Control
The organization: a. Requires personnel to report suspected incidents to the organizational incident response capability within the timeframe established in the current organization Incident Handling Procedure and b. Reports security incident information to designated authorities. **Implementation Standards** 1. Identify the organization's designated security and privacy official(s), if applicable, and/or identify other personnel authorized to access PII and responsible for reporting and managing Incidents or Breaches to CMS; 2. Provide details regarding the identification, response, recovery, and follow-up of Incidents and Breaches, which should include information regarding the potential need for CMS to immediately suspend or revoke access to the Hub for containment purposes; and 3. Require reporting of any security and privacy Incident or Breach of PII to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at cms_it_service_desk@cms.hhs.gov within one hour after discovery of the Incident or Breach.
Related Control Requirement(s): IR-7
Control Implementation Description: "Click here and type text"

14.8.6.1 IR-6 (1): Automated Reporting

IR-6 (1): Automated Reporting
Control
The organization employs automated mechanisms to assist in the reporting of security incidents.
Related Control Requirement(s): IR-7
Control Implementation Description: "Click here and type text"

14.8.7 IR-7: Incident Response Assistance

IR-7: Incident Response Assistance
Control
The organization provides an incident response support resource integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

IR-7: Incident Response Assistance
Related Control Requirement(s): AT-2, IR-4, IR-6, IR-8, SA-9
Control Implementation Description: "Click here and type text"

14.8.7.1 IR-7 (1): Automation Support for Availability of Information / Support

IR-7 (1): Automation Support for Availability of Information / Support	
Control	
The organization employs automated mechanisms to increase the availability of incident response-related information and support.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	

14.8.8 IR-8: Incident Response Plan

IR-8: Incident Response Plan
Control
The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; 8. Is reviewed and approved by the applicable Incident Response Team Leader; b. Distributes copies of the incident response plan to: 1. Chief Information Security Officer; 2. Chief Information Officer; 3. Information System Security Officer; 4. Office of the Inspector General/Computer Crimes Unit; 5. All personnel within the organization Incident Response Team; 6. All personnel within the PII Breach Response Team; and 7. All personnel within the organization Operations Centers. c. Reviews within every three hundred sixty-five (365) days; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to the organizational elements listed in b. above; and f. Protects the incident response plan from unauthorized disclosure and modification.
Related Control Requirement(s): MP-2, MP-4, MP-5
Control Implementation Description: "Click here and type text"

14.8.9 IR-9: Information Spillage Response

IR-9: Information Spillage Response
Control
The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination; b. Alerting incident response personnel (as defined in the applicable security plan) and the incident response plan [See IR-6]) of the information spill using a method of communication not associated with the spill; c. Isolating the contaminated information system or system component;

IR-9: Information Spillage Response
d. Eradicating the information from the contaminated information system or component; e. Identifying other information systems or system components that may have been subsequently contaminated; and f. Performing required response actions as in the system incident response plan.
Related Control Requirement(s): CP-4, IR-6, IR-8
Control Implementation Description: "Click here and type text"

14.9 Maintenance (MA)

14.9.1 MA-1: System Maintenance Policy and Procedures

MA-1: System Maintenance Policy and Procedures
Control
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls. b. Reviews and updates (as necessary) the current: 1. System maintenance policy within every three (3) years; and 2. System maintenance procedures within every three (3) years. c. System maintenance policy and procedures must ensure that contractors having access to records (i.e., files or data) maintained in a system of records are contractually bound to be covered by the Privacy Act.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.9.2 MA-2: Controlled Maintenance

MA-2: Controlled Maintenance
Control
The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

MA-2: Controlled Maintenance
c. Requires that the applicable business owner (or an official designated in the applicable security plan) explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes defined maintenance-related information (defined in the applicable security plan) in organizational maintenance records.
Related Control Requirement(s): CM-3, CM-4, MA-4, MP-6, SI-2
Control Implementation Description: "Click here and type text"

14.9.3 MA-3: Maintenance Tools

MA-3: Maintenance Tools
Control
The organization approves, controls, and monitors information system maintenance tools.
Related Control Requirement(s): MA-2, MA-5, MP-6
Control Implementation Description: "Click here and type text"

14.9.3.1 MA-3 (1): Inspect Tools

MA-3 (1): Inspect Tools
Control
The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.
Related Control Requirement(s): SI-7
Control Implementation Description: "Click here and type text"

14.9.3.2 MA-3 (2): Inspect Media

MA-3 (2): Inspect Media
Control
The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.
Related Control Requirement(s): SI-3
Control Implementation Description: "Click here and type text"

14.9.3.3 MA-3 (3): Prevent Unauthorized Removal

MA-3 (3): Prevent Unauthorized Removal
Control
The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: a. Verifying that there is no organizational or sensitive information contained on the equipment; b. Sanitizing or destroying the equipment; c. Retaining the equipment within the facility; or d. Obtaining an exemption, in writing, from the organization CIO or his/her designated representative explicitly authorizing removal of the equipment from the facility.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.9.4 MA-4: Nonlocal Maintenance

MA-4: Nonlocal Maintenance
Control
The organization monitors and controls nonlocal maintenance and diagnostic activities; and prohibits nonlocal system maintenance unless explicitly authorized, in writing, by the organization CIO or his/her designated representative. If nonlocal maintenance and diagnostic actives are authorized, the organization: a. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; b. Employs strong identification and authentication techniques in the establishment of nonlocal maintenance and diagnostic sessions; c. Maintains records for nonlocal maintenance and diagnostic activities; and d. Terminates all sessions and network connections when nonlocal maintenance is completed. **Implementation Standards** 1. If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service.

MA-4: Nonlocal Maintenance
2. Media used during remote maintenance must be sanitized in accordance with NIST SP 800-88, as amended.
Related Control Requirement(s): AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, MP-6, PL-2, SC-7, SC-10, SC-17
Control Implementation Description: "Click here and type text"

14.9.4.1 MA-4 (1): Auditing and Review

MA-4 (1): Auditing and Review
Control
The organization: a. Audits nonlocal maintenance and diagnostic sessions using available audit events; and b. Reviews the records of the maintenance and diagnostic sessions.
Related Control Requirement(s): AU-2, AU-6, AU-12
Control Implementation Description: "Click here and type text"

14.9.4.2 MA-4 (2): Document Nonlocal Maintenance

MA-4 (2): Document Nonlocal Maintenance
Control
The organization documents in the information system's security plan the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.9.5 MA-5: Maintenance Personnel

MA-5: Maintenance Personnel
Control
The organization: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;

MA-5: Maintenance Personnel
b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
Related Control Requirement(s): AC-2, IA-8, MP-2, PE-2, PE-3, PE-4, RA-3, SA-4, AR-3
Control Implementation Description: "Click here and type text"

14.9.6 MA-6: Timely Maintenance

MA-6: Timely Maintenance
Control
The organization obtains maintenance support and/or spare parts for defined key information system components (defined in the applicable security plan) within the applicable Recovery Time Objective (RTO) specified in the contingency plan. **Implementation Standard** The organization defines a list of security-critical information system components and/or key information technology components.
Related Control Requirement(s): CM-8, CP-2, CP-7, SA-15
Control Implementation Description: "Click here and type text"

14.10 Media Protection (MP)

14.10.1 MP-1: Media Protection Policy and Procedures

MP-1: Media Protection Policy and Procedures
Control
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls. b. Reviews and updates (as necessary) the current: 1. Media protection policy within every three (3) years; and 2. Media protection procedures within every three (3) years. *"Applicable personnel," as referred to in MP-1(a), includes employees and contractors with potential access to personally identifiable information (PII).*

MP-1: Media Protection Policy and Procedures
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.10.2 MP-2: Media Access

MP-2: Media Access
Control
The organization restricts access to sensitive information, such as Personally Identifiable Information (PII), residing on digital and non-digital media to authorized individuals using automated mechanisms to control access to media storage areas in compliance with the latest revision of NIST SP 800-88, Guidelines for Media Sanitization, to defined personnel or roles (defined personnel or roles must be authorized individuals with a valid need to know as defined in the applicable security plan) by disabling: a. CD/DVD writers and allowing access to using CD/DVD viewing and downloading capabilities only to persons specified or in defined roles; and b. USB ports and allowing access to using USB device capabilities only to persons specified or in defined roles. **Implementation Standards** 1. The organization defines types of digital (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, and digital video disks) and non-digital media (e.g., paper, microfilm) and non-digital media. 2. Define a list of individuals with authorized access to defined media types. 3. Define the types of security measures to be used in protecting defined media types.
Related Control Requirement(s): AC-2, AC-3, IA-2, MP-4, PE-2, PE-3, PL-2
Control Implementation Description: "Click here and type text"

14.10.3 MP-3: Media Marking

MP-3: Media Marking
Control
The organization: a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Does not exempt any removable media types from marking
Related Control Requirement(s): PL-2, RA-3
Control Implementation Description: "Click here and type text"

14.10.4 MP-4: Media Storage

MP-4: Media Storage
Control
The organization: a. Physically controls and securely stores all magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks within organization-defined controlled areas); encrypts digital media via a FIPS 140-2 validated encryption module; and for non-digital media, provides secure storage in locked cabinets or safes. b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. **Implementation Standards** 1. If PII is recorded on magnetic media with other data, the media should be protected as if all the data contained consisted of personally identifiable information. 2. Define controlled areas within facilities where the information and information system reside.
Related Control Requirement(s): CP-6, CP-9, MP-2, MP-7, PE-3
Control Implementation Description: "Click here and type text"

14.10.5 MP-5: Media Transport

MP-5: Media Transport
Control
The organization: a. Protects and controls digital and non-digital media defined within the latest revision of NIST SP 800-88, Guidelines for Media Sanitization containing sensitive information during transport outside of controlled areas using cryptography and tamper evident packaging, and; 1. if hand carried, using a securable container (e.g., locked briefcase) via authorized personnel, or 2. if shipped, trackable with receipt by commercial carrier. b. Maintains accountability for information system media during transport outside of controlled areas; c. Documents activities associated with the transport of information system media; and d. Restricts the activities associated with the transport of information system media to authorized personnel. e. Protects and controls digital media that contains personally identifiable information (PII) during transport outside of controlled areas using FIPS 140-2 validated encryption. **Implementation Standards** 1. Protect and control non-digital PII media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. Non-digital PII must be in locked cabinets or sealed packing cartons while in transit. 2. Protect and control magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks during transport outside of controlled areas; and during transport by encrypted digital media using a FIPS 140-2 validated module. 3. Define security measures to protect digital and non-digital media in transport.

MP-5: Media Transport
Related Control Requirement(s): AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28
Control Implementation Description: "Click here and type text"

14.10.5.1 MP-5 (4): Cryptographic Protection

MP-5 (4): Cryptographic Protection
Control
The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.
Related Control Requirement(s): CP-9, MP-2
Control Implementation Description: "Click here and type text"

14.10.6 MP-6: Media Sanitization

MP-6: Media Sanitization
Control
The organization: a. Sanitizes both digital and non-digital information system media prior to disposal, release out of organizational control, or release for reuse using defined sanitization techniques and procedures (defined in the applicable security plan in accordance with the latest revision of NIST SP 800-88, Guidelines for Media Sanitization; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. **Implementation Standards** 1. Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures. 2. Surplus equipment is stored securely while not in use, and disposed of or sanitized in accordance with NIST 800-88 when no longer required. 3. Support the capability to sanitize disk space when released from an instance (container) image file.
Related Control Requirement(s): MA-2, MA-4, RA-3, SC-4, DM-2
Control Implementation Description: "Click here and type text"

14.10.7 MP-7: Media Use

MP-7: Media Use
Control
The organization a. Prohibits the use of personally owned media on organizational information systems or system components using defined security safeguards (defined in the applicable security plan). b. Restricts the use of portable storage and mobile devices on information systems and networks containing PII, without using device ownership, media sanitization and encryption controls.
Related Control Requirement(s): AC-19, PL-4, SE-2
Control Implementation Description: "Click here and type text"

14.10.7.1 MP-7 (1): Prohibit Use Without Owner

MP-7 (1): Prohibit Use Without Owner
Control
The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.
Related Control Requirement(s): PL-4
Control Implementation Description: "Click here and type text"

14.11 Physical and Environmental Protection (PE)

14.11.1 PE-1: Physical and Environmental Protection Policy and Procedures

PE-1: Physical and Environmental Protection Policy and Procedures
Control
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. b. Reviews and updates (as necessary) the current: 1. Physical and environmental protection policy within every three (3) years; and 2. Physical and environmental protection procedures within every three (3) years.

PE-1: Physical and Environmental Protection Policy and Procedures
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.11.2 PE-2: Physical Access Authorizations

PE-2: Physical Access Authorizations
Control
The organization: a. Develops and maintains a current list of individuals with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); b. Issues authorization credentials for facility access; c. Reviews and approves the access list detailing authorization credentials in accordance with the frequency specified in Implementation Standard 1, removing from the access list those personnel no longer requiring access. **Implementation Standards** 1. Review and approve lists of personnel with authorized access to facilities containing information systems at least once every one-hundred eighty (180) days. 2. Create a restricted area, security room, or locked room to control access to areas containing Personally Identifiable Information (PII). These areas will be controlled accordingly.
Related Control Requirement(s): PE-3, PE-4, PS-3
Control Implementation Description: "Click here and type text"

14.11.2.1 PE-2 (1): Access by Position / Role

PE-2 (1): Access by Position / Role
Control
The organization authorizes physical access to the facility where the information system resides based on position or role.
Related Control Requirement(s): AC-2, AC-3, AC-6
Control Implementation Description: "Click here and type text"

14.11.3 PE-3: Physical Access Control

PE-3: Physical Access Control
Control
The organization: a. Enforces physical access authorizations at defined entry/exit points to the facility (defined in the applicable security plan) where the information system resides by: 1. Verifies individual access authorizations before granting access to the facility; 2. Controls entry to the facility containing the information system using guards and/or defined physical access control systems/devices (defined in the applicable security plan); b. Maintains physical access audit logs for defined entry/exit points; c. Escorts visitors and monitors visitor activity in defined circumstances requiring visitor escorts and monitoring (defined in the applicable security plan); d. Secures keys, combinations, and other physical access devices; e. Inventories physical access devices within every 90 days: and f. Changes combinations and keys for defined high-risk entry/exit points (defined in the applicable security plan) within every three hundred sixty-five (365) days, and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated. **Implementation Standards** 1. Control data center/facility access by use of door and window locks, and security personnel or physical authentication devices, such as biometrics and/or smart card/PIN combination. 2. Store and operate servers in physically secure environments, and grant access to explicitly authorized personnel only. Access is monitored and recorded. 3. Restrict access to grounds/facilities to authorized persons only. 4. Require two barriers to access Personally Identifiable Information (PII) under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Protected information must be containerized in areas where other than authorized employees may have access afterhours.
Related Control Requirement(s): AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3
Control Implementation Description: "Click here and type text"

14.11.4 PE-4: Access Control for Transmission Medium

PE-4: Access Control for Transmission Medium
Control
The organization controls physical access to information system distribution and transmission lines within organizational facilities. **Implementation Standard** Disable any physical ports (e.g., wiring closets and patch panels) not in use.

PE-4: Access Control for Transmission Medium
Related Control Requirement(s): MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8
Control Implementation Description: "Click here and type text"

14.11.5 PE-5: Access Control for Output Devices

PE-5: Access Control for Output Devices
Control
The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.
Related Control Requirement(s): PE-2, PE- 3, PE-4,
Control Implementation Description: "Click here and type text"

14.11.6 PE-6: Monitoring Physical Access

PE-6: Monitoring Physical Access
Control
The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs at least semi-annually and upon occurrence of security incidents involving physical security; and c. Coordinates results of reviews and investigations with the organization's incident response capability. **Implementation Standard** The organization reviews physical access logs at least semi-annually.
Related Control Requirement(s): CA-7, IR-4, IR-8
Control Implementation Description: "Click here and type text"

14.11.6.1 PE-6 (1): Intrusion Alarms / Surveillance Equipment

PE-6 (1): Intrusion Alarms/Surveillance Equipment
Control
The organization monitors physical intrusion alarms and surveillance equipment.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.11.7 PE-8: Visitor Access Records

PE-8: Visitor Access Records
Control
The organization: a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) for two (2) years; and b. Reviews visitor access records at least monthly. **Implementation Standards** At a minimum, visitor access records must include the following information: a. Name and organization of the person visiting; b. Visitor's signature; c. Form of identification; d. Date of access; e. Time of entry and departure; f. Purpose of visit; and g. Name and organization of person visited.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.12 Planning (PL)

14.12.1 PL-1: Security Planning Policy and Procedures

PL-1: Security Planning Policy and Procedures
Control
The organization: a. Develops, documents, and disseminates to applicable personnel:

PL-1: Security Planning Policy and Procedures
1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls. b. Reviews and updates (as necessary) the current: 1. Security planning policy within every three (3) years; and 2. Security planning procedures within every three (3) years.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.12.2 PL-2: System Security Plan

PL-2: System Security Plan
Control
The organization: a. Develops a security plan for the information system that: 1. Is consistent with CMS specified System Security Plan (SSP) Workbook; 2. Is consistent with the organization's enterprise architecture; 3. Explicitly defines the authorization boundary for the system; 4. Describes the operational context of the information system in terms of missions and business processes; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Provides the security category 8. Personally Identifiable information (PII) confidentiality impact level of the system (as described in NIST SP 800-122), 9. Describes relationships with, and data flows of, PII to other systems; and provide an overview of security and privacy requirements for the system 10. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and 11. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distributes copies of the security plan and communicates subsequent changes to the plan to stakeholders; c. Reviews the security plan for the information system within every three hundred sixty-five (365) days; d. Updates the plan, at a minimum every three (3) years, to address current conditions or whenever: 1. There are significant changes to the information system/environment of operation that affect security; 2. Problems are identified during plan implementation or security control assessments; 3. When the data sensitivity level increases; 4. After a serious security violation due to changes in the threat environment; or 5. Before the previous security authorization expires; and e. Protects the security plan from unauthorized disclosure and modification.

PL-2: System Security Plan
Implementation Standard The SSP must define the boundary within the system where PII is stored, processed, and/or maintained. The person responsible for meeting information system privacy requirements must provide input to the SSP.
Related Control Requirement(s): AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-5, SA-5, SA-17
Control Implementation Description: The System Security Plan (SSP) is a required artifact. "Click here and type text"

14.12.2.1 PL-2 (3): Plan / Coordinate with Other Organizational Entities

PL-2 (3): Plan / Coordinate with Other Organizational Entities
Control
The organization plans and coordinates security-related activities regarding the information system with affected stakeholders before conducting such activities to reduce the impact on other organizational entities.
Related Control Requirement(s): CP-4, IR-4
Control Implementation Description: "Click here and type text"

14.12.3 PL-4: Rules of Behavior

PL-4: Rules of Behavior
Control
The organization: a. Establishes and makes readily available to individuals requiring access to the information system the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives an acknowledgment (paper or electronic) from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to information and the information system; c. Reviews the rules of behavior every three hundred sixty-five (365) days, updating if necessary; and d. Requires individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules of behavior are revised/updated. e. Informs employees and contractors that the use of the organization's information resources for anything other than authorized purposes set forth in the RoB is a violation of the policy, and is grounds for disciplinary action, monetary fines, and/or criminal charges that could result in imprisonment; and f. Informs employees and contractors that the use of the organization's information resources is subject to the organization's monitoring of employee use of organizational information resources.

PL-4: Rules of Behavior
Related Control Requirement(s): AC-2, AC-6, AC-8, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5, AR-5
Control Implementation Description: "Click here and type text"

14.12.3.1 PL-4 (1): Social Media and Networking Restrictions

PL-4 (1): Social Media and Networking Restrictions
Control
The organization includes in the rules of behavior explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.12.4 PL-8: Information Security Architecture

PL-8: Information Security Architecture
Control
The organization: a. Develops an information security architecture for the ACA system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates (as necessary) the information security architecture whenever changes are made to the enterprise architecture; and c. Ensures that planned information security architecture changes are reflected in the security plan and organizational procurements/acquisitions.
Related Control Requirement(s): CM-2, CM-6, PL-2, SA-5, SA-17
Control Implementation Description: "Click here and type text"

14.13 Personnel Security (PS)

14.13.1 PS-1: Personnel Security Policy and Procedures

PS-1: Personnel Security Policy and Procedures
Control
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. b. Reviews and updates (as necessary) the current: 1. Personnel security policy within three (3) years; and 2. Personnel security procedures within every three (3) years.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.13.2 PS-2: Position Risk Designation

PS-2: Position Risk Designation
Control
The organization: a. Assigns a criticality/sensitivity risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position criticality/sensitivity risk designations within every three years.
Related Control Requirement(s): AT-3, PL-2, PS-3
Control Implementation Description: "Click here and type text"

14.13.3 PS-3: Personnel Screening

PS-3: Personnel Screening
Control
The organization: a. Screens individuals prior to authorizing access to the information system; b. Rescreens individuals periodically, consistent with the criticality/sensitivity risk designation of the position; and

PS-3: Personnel Screening
c. When an employee moves from one position to another, the higher level of clearance should be adjudicated. **Implementation Standards** 1. Perform criminal history check for all persons prior to employment. 2. All employees and contractors requiring access to ACA-sensitive information must meet personnel suitability standards. These suitability standards are based on a valid need-to-know, which cannot be assumed from position or title, and favorable results from a background check. The background check for prospective and existing employees (if not previously completed) should include, at a minimum, contacting references provided by the employee as well as the local law enforcement agency or agencies.
Related Control Requirement(s): AC-2, IA-4. PE-2, PS-2
Control Implementation Description: "Click here and type text"

14.13.4 PS-4: Personnel Termination

PS-4: Personnel Termination
Control
The organization, upon termination of individual employment: a. Disables information system access in accordance with Implementation Standard 1; b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of non-disclosure of information security and privacy information; d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by a terminated individual; f. Notifies defined personnel or roles (defined in the applicable security plan) within one (1) business day; and g. Immediately escorts employees terminated for cause out of the organization. **Implementation Standards** 1. System and physical access must be revoked prior to or during the employee termination process. 2. All access and privileges to systems, networks, and facilities are suspended when employees or contractors temporarily separate from the organization (e.g., leave of absence).
Related Control Requirement(s): AC-2, IA-4, PE-2, PS-5, PS-6
Control Implementation Description: "Click here and type text"

14.13.5 PS-5: Personnel Transfer

PS-5: Personnel Transfer
Control
The organization: a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiates the following transfer or reassignment actions during the formal transfer process: 1. Re-issuing appropriate information system-related property (e.g., keys, identification cards, and building passes); 2. Notification to security management; 3. Closing obsolete accounts and establishing new accounts; 4. When an employee moves to a new position of trust, logical and physical access controls must be re-evaluated within five (5) days following the formal transfer action; c. Modifies access authorization as necessary to correspond with any changes in operational need due to reassignment or transfer; and d. Notifies defined personnel or roles (defined in the applicable security plan) within one (1) business day.
Related Control Requirement(s): AC-2, IA-4, PE-2, PS-4
Control Implementation Description: "Click here and type text"

14.13.6 PS-6: Access Agreements

PS-6: Access Agreements
Control
The organization: a. Develops and documents access agreements for organizational information systems, consistent with the provisions of the ACA and the requirements of 45 CFR §155.260 – Privacy and security of personally identifiable information, paragraphs (b)(2) and (c). b. Reviews and updates the access agreements as part of the system security authorization or when a contract is renewed or extended, but minimally within every three hundred sixty-five (365) days, whichever occurs first; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Acknowledge (paper or electronic) appropriate access agreements prior to being granted access; and 2. Re-acknowledge access agreements to maintain access to organizational information systems when access agreements have been updated or with in every 365 days.
Related Control Requirement(s): PL-4, PS-2, PS-3, PS-4, PS-8
Control Implementation Description: "Click here and type text"

14.13.7 PS-7: Third-Party Personnel Security

PS-7: Third-Party Personnel Security
Control
The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify Contracting Officers or Contracting Officer's Representatives (via the roster of contractor personnel) of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within seven (7) calendar days; and e. Monitors provider compliance. **Implementation Standards** Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support information security policies and standards.
Related Control Requirement(s): PS-2, PS-3, PS-4, PS-5, PS-6, SA-9
Control Implementation Description: "Click here and type text"

14.13.8 PS-8: Personnel Sanctions

PS-8: Personnel Sanctions
Control
The organization: a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notifies defined personnel or roles (defined in the applicable security plan) within defined time period (defined in the applicable security plan) not to exceed seven (7) calendar days when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.
Related Control Requirement(s): PL-4, PS-6
Control Implementation Description: "Click here and type text"

14.14 Risk Assessment (RA)

14.14.1 RA-1: Risk Assessment Policy and Procedures

RA-1: Risk Assessment Policy and Procedure
Control
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls on information systems and paper records; and b. Reviews and updates (as necessary) the current: 1. Risk assessment policy within every three (3) years and 2. Risk assessment procedures within every three (3) years.
Related Control Requirement(s): AR-2
Control Implementation Description: "Click here and type text"

14.14.2 RA-3: Risk Assessment

RA-3: Risk Assessment
Control
The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in the applicable security plan; c. Reviews risk assessment results within every three hundred sixty-five (365) days; d. Disseminates risk assessment results to affected stakeholders and Business Owners(s); and e. Updates the risk assessment every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system. **Implementation Standard** The organization conducts an information security risk assessment and documents risk assessment results.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.14.3 RA-5: Vulnerability Scanning

RA-5: Vulnerability Scanning
Control
The organization: a. Scans for vulnerabilities in the information system and hosted applications, operating system, web application, and database scans (as applicable) within every thirty (30) days and when new critical or high vulnerabilities potentially affecting the system/applications are identified and reported no less than 72 hours; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with affected/related stakeholders on a "need to know" basis to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). **Implementation Standards** 1. Vulnerability scans must be performed when new vulnerabilities, risks, or threats potentially affecting the system/applications are identified and reported. 2. Raw results from vulnerability scanning tools must be available in an unaltered format to the organization, 3. The organization must provide timely responses to informational requests for organizational monitoring status and security posture information.
Related Control Requirement(s): CA-2, CA-7, CM-4, CM-6, RA-3, SA-11, SI-2
Control Implementation Description: "Click here and type text"

14.14.3.1 RA-5 (1): Update Tool Capability

RA-5 (1): Update Tool Capability
Control
The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities scanned.
Related Control Requirement(s): SI-3, SI-7
Control Implementation Description: "Click here and type text"

14.14.3.2 RA-5 (2): Update by Frequency / Prior to New Scan / When Identified

RA-5 (2): Update by Frequency / Prior to New Scan / When Identified
Control
The organization updates the information system vulnerabilities scanned within every thirty (30) days, no less often than before each scan or when new vulnerabilities are identified and reported.
Related Control Requirement(s): SI-3, SI-5
Control Implementation Description: "Click here and type text"

14.14.3.3 RA-5 (5): Privileged Access

RA-5 (5): Privileged Access
Control
The information system implements privileged access authorization to operating system, telecommunications, and configuration components for selected vulnerability scanning activities to facilitate more thorough scanning. **Implementation Standards** 1. If Automated scanning tool functionality is used, it must be able to perform credentialed scans. 2. Credentialed scanning must be performed on all information systems and network devices (including appliances) 3. The organization must maintain and provide changes to the system accounts to support credentialed scanning no later than two (2) weeks prior to expiration or when other changes to the accounts are needed.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.15 System and Services Acquisition (SA)

14.15.1 SA-1: System and Services Acquisition Policy and Procedures

SA-1: System and Services Acquisition Policy and Procedures
Control
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and updates (as necessary) the current: 1. System and services acquisition policy within every three (3) years; and 2. System and services acquisition procedures within every three (3) years.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.15.2 SA-2: Allocation of Resources

SA-2: Allocation of Resources
Control
The organization: a. Determines information security requirements for the information system or information system service in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; 1. As part of the capital planning and investment control process, the organization must determine, document, and allocate resources required to protect the privacy and confidentiality of personally identifiable information (PII) in the information system. c. Includes information security requirements in mission/business case planning, and d. Establishes a discrete line item in programming and budgeting documentation for the implementation and management of information systems security.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.15.3 SA-3: System Development Life Cycle

SA-3: System Development Life Cycle	
Control	
The organization: a. Manages the information system using the organization-defined system development life cycle (SDLC) that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the system development life cycle; c. Identifies individuals having information system security roles and responsibilities; and d. Integrates the organizational information security risk management process into system development life cycle activities.	
Related Control Requirement(s):	AT-3, SA-8, AR-7
Control Implementation Description: "Click here and type text"	

14.15.4 SA-4: Acquisition Process

SA-4: Acquisition Process
Control
The organization: a. Includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: 1. Security functional requirements; 2. Security strength requirements; 3. Security assurance requirements; 4. Security-related documentation requirements; 5. Requirements for protecting security-related documentation; 6. Description of the information system development, implementation and production environments or their equivalents; 7. Acceptance criteria b. When acquiring information systems, components, or services used to store, process, or transmit personally identifiable information (PII), ensure the following, in consultation with the privacy office, are included in the acquisition contract: 1. List of security and privacy controls necessary to ensure protection of PII and, if appropriate, enforce applicable privacy requirements. 2. Privacy requirements set forth in Appendix J of NIST SP 800-53, Rev. 4, including privacy training and awareness, and rules of behavior. 3. Privacy functional requirements, i.e., functional requirements specific to privacy. 4. Privacy Act of 1974 and any other organization-specific privacy clauses.

SA-4: Acquisition Process
Related Control Requirement(s): CM-6, PS-7, SA-3, SA-5, SA-8, SA-11
Control Implementation Description: "Click here and type text"

14.15.4.1 SA-4 (1): Functional Properties of Security Controls

SA-4 (1): Functional Properties of Security Controls
Control
The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.
Related Control Requirement(s): SA-5
Control Implementation Description: "Click here and type text"

14.15.4.2 SA-4 (2): Design / Implementation Information for Security Controls

SA-4 (2): Design / Implementation Information for Security Controls
Control
The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: a. Security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces; b. Source code and hardware schematics; and c. High-level design documentation at sufficient detail to prove the security control implementation.
Related Control Requirement(s): SA-5
Control Implementation Description: "Click here and type text"

14.15.4.3 SA-4 (9): Functions / Ports / Protocols / Services in Use

SA-4 (9): Functions / Ports / Protocols / Services in Use
Control
The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle the functions, ports, protocols, and services intended for organizational use.

SA-4 (9): Functions / Ports / Protocols / Services in Use
Related Control Requirement(s): CM-7, SA-9
Control Implementation Description: "Click here and type text"

14.15.5 SA-5: Information System Documentation

SA-5: Information System Documentation
Control
The organization: a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; b. Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent, and evaluate whether such documentation is essential for the effective implementation or operation of security controls; d. Protects documentation as required, in accordance with the risk management strategy; and e. Distributes documentation to defined personnel or roles (defined in the applicable system security plan [SSP]).
Related Control Requirement(s): CM-6, CM-8, PL-4, PS-2, SA-3, SA-4
Control Implementation Description: "Click here and type text"

14.15.6 SA-8: Security Engineering Principles

SA-8: Security Engineering Principles
Control
The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

SA-8: Security Engineering Principles
Related Control Requirement(s): SA-3, SA-4, SC-2
Control Implementation Description: "Click here and type text"

14.15.7 SA-9: External Information System Services

SA-9: External Information System Services
Control The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities regarding external information system services in a SLA or similar agreement; and c. Employs defined processes, methods, and techniques (defined in the applicable system security plan [SSP]) to monitor security control compliance by external service providers on an ongoing basis.
Related Control Requirement(s): CA-3, IR-7, PS-7
Control Implementation Description: "Click here and type text"

14.15.8 SA-10: Developer Configuration Management

SA-10: Developer Configuration Management
Control
The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service development, implementation, and operation; b. Document, manage, and control the integrity of changes to configuration items under configuration management; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to defined personnel or roles (defined in the applicable system security plan [SSP]).
Related Control Requirement(s): CM-3, CM-4, CM-9, SI-2
Control Implementation Description: "Click here and type text"

14.15.9 SA-11: Developer Security Testing and Evaluation

SA-11: Developer Security Testing and Evaluation
Control
The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan that includes assessment of privacy controls in accordance with, but not limited to, current organization procedures; b. Perform unit; integration; system; regression testing/evaluation in accordance with organizational defined system development life cycle; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation. f. Conduct tests that: 1. Minimize to the use of PII to the maximum extent practicable; 2. Use actual PII only if a formal memorandum of agreement (MOA), memorandum of understanding (MOU), or data exchange agreement has been established between the data owner of the PII and the entity developing/testing the information system including how loss, theft, or compromise (i.e., breach) of PII is to be handled; 3. Use de-identified or anonymized PII to the maximum extent practicable; and 4. Coordinate use of PII with the organization's privacy office before conducting any testing. **Implementation Standards** 1. If the security control assessment results are used in support of the security authorization process for the information system, ensure that no security relevant modifications of the information systems have been made subsequent to the assessment and after selective verification of the results. 2. Use hypothetical data when executing test scripts or in a test environment that is configured to comply with the security controls as if it is a production environment. 3. All systems supporting development and pre-production testing are connected to an isolated network separated from production systems. Network traffic into and out of the development and pre-production testing environment is only permitted to facilitate system testing, and is restricted by source and destination access control lists as well as ports and protocols.
Related Control Requirement(s): CA-2, CM-4, SA-3, SA-4, SA-5, SI-2
Control Implementation Description: "Click here and type text"

14.15.10 SA-15: Development Process, Standards, and Tools

SA-15: Development Process, Standards, and Tools
Control
The organization: a. Requires the developer of the information system, system component, or information system service to follow a documented development process that: 1. Explicitly addresses security requirements;

SA-15: Development Process, Standards, and Tools
2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Reviews the development process, standards, tools, and tool options/configurations at least every three (3) years to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy all applicable System Acquisition (SA) and Configuration Management (CM) security controls
Related Control Requirement(s): SA-3, SA-8
Control Implementation Description: "Click here and type text"

14.15.11 SA-17: Developer Security Architecture and Design

SA-17: Developer Security Architecture and Design
Control
The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that: a. Is consistent with and supportive of the organization's security architecture (see PL-8), which is established within and is an integrated part of the organization's enterprise architecture; and b. Accurately and completely describes the required security functionality and the allocation of security controls among physical and logical components; and c. Accurately and completely describes the privacy requirements and the allocation of security and privacy controls among physical and logical components d. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.
Related Control Requirement(s): PL-8, SA-3, SA-8, AR-7
Control Implementation Description: "Click here and type text"

14.15.12 SA-22: Unsupported System Components

SA-22: Unsupported System Components
Control
The organization: a. Replaces information system components as soon as possible after discovery that support for the components is no longer available from the developer, vendor, or manufacturer, and b. Where immediate replacement is not possible, provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

SA-22: Unsupported System Components
Related Control Requirement(s): PL-2, SA-3
Control Implementation Description: "Click here and type text"

14.16 System and Communications Protection (SC)

14.16.1 SC-1: System and Communications Protection Policy and Procedures

SC-1: System and Communications Protection Policy and Procedures
Control
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates (as necessary) the current: 1. System and communications protection policy within every three (3) years; and 2. System and communications protection procedures within every three (3) years.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.16.2 SC-2: Application Partitioning

SC-2: Application Partitioning
Control
a. The information system separates user functionality (including user interface services) from information system management functionality. b. In any situation where personally identifiable information (PII) is present, PII must be stored on a logical or physical partition separate from the applications and software partition.
Related Control Requirement(s): SA-4, SA-8
Control Implementation Description: "Click here and type text"

14.16.3 SC-4: Information in Shared Resources

SC-4: Information in Shared Resources
Control
The information system prevents unauthorized and unintended information transfer via shared system resources. **Implementation Standards** 1. Ensure that users of shared system resources cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user. 2. Ensure that system resources shared between two (2) or more users are released back to the information system and are protected from accidental or purposeful disclosure.
Related Control Requirement(s): AC-3, AC-4, MP-6
Control Implementation Description: "Click here and type text"

14.16.4 SC-5: Denial of Service Protection

SC-5: Denial of Service Protection
Control
The information system protects against or limits the effects of the types of denial of service attacks defined in NIST SP 800-61, Computer Security Incident Handling Guide, and the following websites by employing defined security safeguards (defined in the applicable system security plan): • SANS Organization: www.sans.org/dosstep; • SANS Organization's Roadmap to Defeating DDoS: www.sans.org/dosstep; and • NIST National Vulnerability Database: http://nvd.nist.gov/cvss.cfm. **Implementation Standards** The organization defines a list of types of denial of service attacks (including but not limited to flooding attacks and software/logic attacks) or provides a reference to source for current list.
Related Control Requirement(s): SC-6, SC-7
Control Implementation Description: "Click here and type text"

14.16.5 SC-6: Resource Availability

SC-6: Resource Availability
Control
The information system protects the availability of resources by allocating resources by priority and/or quota.
Related Control Requirement(s):

SC-6: Resource Availability
Control Implementation Description:
"Click here and type text"

14.16.6 SC-7: Boundary Protection

SC-7: Boundary Protection
Control
The information system: a. Monitors and controls communications at the external boundary, both physically and logically, of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. **Implementation Standards** 1. Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required. 2. Utilize stateful inspection/application firewall hardware and software. 3. Utilize firewalls from two (2) or more different vendors at the various levels within the network to reduce the possibility of compromising the entire network. 4. If the system has an outward facing Web or email presence to the public internet, the organization must implement and support a technical capability to detect malware in web traffic traversing the organization's boundary by: a. Monitoring assets without the need to deploy software agents (zero client footprint); b. Dynamically generating actionable malware intelligence; c. Detecting and stopping web-based and email attacks; and d. Sending alert data to the organization's SIEM. 5. Aggregated boundary protection device information must be searchable by the organization: a. Information is provided to the organization in a format compliant with organization (e.g., Continuous Diagnostics and Mitigation) requirements; b. Information sources include boundary protection systems, appliances, devices, services, and applications; and c. Organization directed aggregated boundary protection device information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. 6. As required by the organization, raw boundary protection device information from relevant automated tools must be available in an unaltered format to the organization.
Related Control Requirement(s):
AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13
Control Implementation Description:
"Click here and type text"

14.16.6.1 SC-7 (3): Access Points

SC-7 (3): Access Points
Control
The organization limits the number of external network connections to the information system.

SC-7 (3): Access Points
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.16.6.2 SC-7 (4): External Telecommunications Services

SC-7 (4): External Telecommunications Services
Control
The organization: a. Implements a managed interface for each external telecommunication service; b. Establishes a traffic flow policy for each managed interface; c. Protects the confidentiality and integrity of the information being transmitted across each interface; d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and e. Reviews exceptions to the traffic flow policy within every three hundred sixty-five (365) days or implementation of major new system, and removes exceptions that are no longer supported by an explicit mission/business need.
Related Control Requirement(s): SC-8
Control Implementation Description: "Click here and type text"

14.16.6.3 SC-7 (5): Deny by Default / Allow by Exception

SC-7 (5): Deny by Default / Allow by Exception
Control
The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.16.6.4 SC-7 (7): Prevent Split Tunneling for Remove Devices

SC-7 (7): Prevent Split Tunneling for Remove Devices
Control
The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.16.6.5 SC-7 (8): Route Traffic to Authenticated Proxy Servers

SC-7 (8): Route Traffic to Authenticated Proxy Servers
Control
The information system routes all user-initiated internal communications traffic to untrusted external networks through authenticated proxy servers at managed interfaces. **Implementation Standard** The organization defines the internal communications traffic to be routed by the information system through authenticated proxy servers and the external networks that are the prospective destination of such traffic routing.
Related Control Requirement(s): AC-3, AU-2
Control Implementation Description: "Click here and type text"

14.16.6.6 SC-7 (12): Host-Based Protection

SC-7 (12): Host-Based Protection
Control
The organization implements defined, host-based boundary protection mechanisms at defined information system components, including servers, workstations, and mobile devices.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.16.6.7 SC-7 (13): Isolation of Security Tools / Mechanisms / Support Components

SC-7 (13): Isolation of Security Tools / Mechanisms / Support Components
Control
The organization defines key information security tools, mechanisms, and support components associated with system and security administration; and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.
Related Control Requirement(s): SA-8, SC-2
Control Implementation Description: "Click here and type text"

14.16.6.8 SC-7 (18): Fail Secure

SC-7 (18): Fail Secure
Control
The information system fails securely in the event of an operational failure of a boundary protection device.
Related Control Requirement(s): CP-2, SC-24
Control Implementation Description: "Click here and type text"

14.16.7 SC-8: Transmission Confidentiality and Integrity

SC-8: Transmission Confidentiality and Integrity
Control
The information system protects the confidentiality and integrity of information. Any transmitted data containing sensitive information must be encrypted using a FIPS 140-2 validated module. (See SC-13*).*
Related Control Requirement(s): AC-17, PE-4, SI-4, AR-4
Control Implementation Description: "Click here and type text"

14.16.7.1 SC-8 (1): Cryptographic or Alternate Physical Protection

SC-8 (1): Cryptographic or Alternate Physical Protection
Control
The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by approved alternative safeguards and defined in the applicable system security plan and Information System Risk Assessment. FIPS-validated encryption or protected distribution systems are used to protect PII to ensure the information's confidentiality and integrity during transmission.
Related Control Requirement(s): SC-13
Control Implementation Description: "Click here and type text"

14.16.7.2 SC-8 (2): Pre / Post Transmission Handling

SC-8 (2): Pre / Post Transmission Handling
Control
The information system maintains the confidentiality and integrity of information during preparation for transmission and during reception.
Related Control Requirement(s): AU-10
Control Implementation Description: "Click here and type text"

14.16.8 SC-10: Network Disconnect

SC-10: Network Disconnect
Control
The information system: a. Terminates the network connection associated with a communications session at the end of the session, or: 1. Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and 2. Forcibly disconnects inactive VPN connections after thirty (30) minutes or less of inactivity; and b. Terminates or suspends network connections (i.e., a system to system interconnection) upon issuance of an order by the organization CIO, CISO, or Senior Official for Privacy (SOP), **Implementation Standards** 1. The information system terminates the network connection associated with a communications session at the end of the session, or after thirty (30) minutes for all RAS-based sessions and thirty (30) to sixty (60) minutes for non-interactive users, of inactivity. 2. Long running batch jobs and other operations are not subject to this time limit.
Related Control Requirement(s):

SC-10: Network Disconnect
Control Implementation Description: "Click here and type text"

14.16.9 SC-12: Cryptographic Key Establishment and Management

SC-12: Cryptographic Key Establishment and Management
Control
When cryptography is required and used within the information system, the organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with defined requirements (defined in, or referenced by, the applicable security plan) for key generation, distribution, storage, access, and destruction.
Related Control Requirement(s): SC-13, SC-17
Control Implementation Description: "Click here and type text"

14.16.9.1 SC-12 (2): Symmetric Keys

SC-12 (2): Symmetric Keys
Control
The organization produces, controls, and distributes symmetric cryptographic keys using NIST FIPS-compliant key management technology and processes.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.16.10 SC-13: Cryptographic Protection

SC-13: Cryptographic Protection
Control
The information system implements cryptographic mechanisms, in transit and at rest, validated under the Cryptographic Module Validation Program (see http://csrc.nist.gov/groups/STM/cmvp/validation.html), and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

SC-13: Cryptographic Protection
Related Control Requirement(s): AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7
Control Implementation Description: "Click here and type text"

14.16.11 SC-17: Public Key Infrastructure Certificates

SC-17: Public Key Infrastructure Certificates
Control
The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates from an approved service provider.
Related Control Requirement(s): SC-12
Control Implementation Description: "Click here and type text"

14.16.12 SC-18: Mobile Code

SC-18: Mobile Code
Control
The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.
Related Control Requirement(s): AU-2, AU-12, CM-2, CM-6, SI-3
Control Implementation Description: "Click here and type text"

14.16.13 SC-19: Voice Over Internet Protocol

SC-19: Voice Over Internet Protocol
Control
The organization prohibits the use of VoIP technologies, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If VoIP is authorized, the organization:

SC-19: Voice Over Internet Protocol
a. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously; b. Authorizes, monitors, and controls the use of VoIP within the information system; and c. Ensures VoIP equipment used to transmit or discuss sensitive information is protected with organization's (FIPS 140-2 validated module) encryption requirements.
Related Control Requirement(s): CM-6, SC-7
Control Implementation Description: "Click here and type text"

14.16.14 SC-20: Secure Name / Address Resolution Service (Authoritative Source)

SC-20: Secure Name / Address Resolution Service (Authoritative Source)
Control
The information system: a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains when operating as part of a distributed, hierarchical namespace.
Related Control Requirement(s): AU-10, SC-8, SC-12, SC-13, SC-21, SC-22
Control Implementation Description: "Click here and type text"

14.16.15 SC-21: Secure Name / Address Resolution Service (Recursive or Caching Resolver)

SC-21: Secure Name / Address Resolution Service (Recursive or Caching Resolver)
Control
The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.
Related Control Requirement(s): SC-22
Control Implementation Description: "Click here and type text"

14.16.16 SC-22: Architecture and Provisioning for Name / Address Resolution Service

SC-22: Architecture and Provisioning for Name / Address Resolution Service
Control
The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement internal/external role separation.
Related Control Requirement(s): SC-2, SC-21, SC-24
Control Implementation Description: "Click here and type text"

14.16.17 SC-23: Session Authenticity

SC-23: Session Authenticity
Control
The information system protects the authenticity of communications sessions.
Related Control Requirement(s): SC-8, SC-10, SC-11
Control Implementation Description: "Click here and type text"

14.16.18 SC-24: Fail in Known State

SC-24: Fail in Known State
Control
The information system fails to a known secure state for all failures preserving the maximum amount of state information in failure.
Related Control Requirement(s): CP-2, CP-10, SC-7, SC-22
Control Implementation Description: "Click here and type text"

14.16.19 SC-28: Protection of Information at Rest

SC-28: Protection of Information at Rest
Control
The information system protects the confidentiality and integrity of information at rest.

SC-28: Protection of Information at Rest
a. The information system enforces encryption of the instance (container) image files under the hypervisor: b. Instance (container) image files from virtual server and client deployments must be encrypted in a manner that meets FIPS 140-2 validated requirements. **Implementation Standard** The information system supports the capability to use cryptographic mechanisms to protect information at rest.
Related Control Requirement(s): AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7
Control Implementation Description: "Click here and type text"

14.16.20 SC-CMS-1: Electronic Mail

SC-CMS-1: Electronic Mail
Control
Controls must be implemented to protect sensitive information that is sent via email. **Implementation Standards** 1. Email and any attachment that contains sensitive information when transmitted inside and outside of the organization premises shall be encrypted using a FIPS 140-2 validated encryption solution: a. Password protection of files is recommended to add an additional layer of data protection but shall not be used in lieu of encryption solutions. b. Password and/or encryption key shall not be included in the same email that contains sensitive information or in separate email. Password/encryption key shall be provided to the recipient separately via text message, verbally, or other out-of-band solution. 2. Multifactor authentication is recommended before being granted access to the organization email.
Related Control Requirement(s): SI-8
Control Implementation Description: "Click here and type text"

14.17 System and Information Integrity (SI)

14.17.1 SI-1: System and Information Integrity Policy and Procedures

SI-1: System and Information Integrity Policy and Procedures
Control
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and updates (as necessary) the current:

SI-1: System and Information Integrity Policy and Procedures
1. System and information integrity policy at least every three (3) years; and 2. System and information integrity procedures at least every (3) years.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.17.2 SI-2: Flaw Remediation

SI-2: Flaw Remediation
Control
The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation in a test environment for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates as directed in Implementation Standard 1; and d. Incorporates flaw remediation into the organizational configuration management process. **Implementation Standards** 1. Correct identified security-related information system flaws on production equipment within ten (10) business days and all others within thirty (30) calendar days. a. Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes; and b. Manage the flaw remediation process centrally. 2. A risk-based decision is documented through the configuration management process in the form of written authorization from the organization CIO or his/her designated representative (e.g., the system data owner or organization CISO) and updated documentation in the risk analysis and security plan if a security patch is not to be applied to an information technology component or a legacy (no-longer maintained by the vendor) component is to remain in use. 3. Flaw remediation requirements apply to all information technology components for which a patch or work-around exists for each vendor-identified and/or CVE/CWE -identified vulnerability. 4. The organization must provide timely responses, as defined by the CISO, to informational requests for organizational flaw (e.g., patch) status and posture information.
Related Control Requirement(s): CA-2, CA-7, CM-3, CM-5, CM-8, IR-4, MA-2, RA-5, SA-10, SA-11, SI-11
Control Implementation Description: "Click here and type text"

14.17.2.1 SI-2 (2): Automated Flaw Remediation Status

SI-2 (2): Automated Flaw Remediation Status
Control
The organization employs automated mechanisms no less often than once every seventy-two (72) hours to determine the state of information system components regarding flaw remediation.

SI-2 (2): Automated Flaw Remediation Status
Related Control Requirement(s): CM-6, SI-4
Control Implementation Description: "Click here and type text"

14.17.2.2 SI-2 (3): Time to Remediate Flaws / Benchmarks for Corrective Actions

SI-2 (3): Time to Remediate Flaws / Benchmarks for Corrective Actions
Control
The organization: a. Measures the time between flaw identification and flaw remediation; and b. Corrective actions must be taken within the time periods defined under the SI-2 (Flaw Remediation) Implementation Standards.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.17.3 SI-3: Malicious Code Protection

SI-3: Malicious Code Protection
Control
The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organization configuration management policy and procedures; and c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the information system using the frequency specified in Implementation Standard 1 and Implementation Standard 2, and real-time scans of files from external sources at endpoint, and/or network entry/exit points, as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. Block and quarantine malicious code and send alert to administrator in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. **Implementation Standards** 1. Desktop malicious code scanning software is configured to perform critical system file scans no less often than once every twelve (12) hours and full system scans no less often than once every seventy-two (72) hours. 2. Server (to include databases and applications) malicious code scanning software is configured to perform critical system file scans no less often than once every twelve (12) hours and full system scans no less often than once every seventy-two (72) hours.

SI-3: Malicious Code Protection
3. Malicious code scanning results are reported to the organization Security Information and Event Management (SIEM) team in compliance with AU-6.
Related Control Requirement(s): CM-3, MP-2, SA-4, SA-8, SC-7, SI-2, SI-4, SI-7
Control Implementation Description: "Click here and type text"

14.17.3.1 SI-3 (2): Automatic Updates

SI-3 (2): Automatic Updates
Control
The information system automatically updates malicious code protection mechanisms.
Related Control Requirement(s): SI-8
Control Implementation Description: "Click here and type text"

14.17.4 SI-4: Information System Monitoring

SI-4: Information System Monitoring
Control
The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with the organization's incident handling policy and procedure; and 2. Unauthorized local, network, and remote connections twice weekly; b. Identifies unauthorized use of the information system through defined techniques and methods (defined in the applicable System Security Plan); c. Deploys monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization. d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, and other organizations based on law enforcement information or other credible sources of information; f. Obtains legal opinion about information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides defined information system monitoring information (defined in the applicable System Security Plan) to defined personnel or roles (defined in the applicable System Security Plan) as needed, and at defined frequency (defined in the applicable System Security Plan).

SI-4: Information System Monitoring
Implementation Standards 1. Implement a centrally managed Intrusion Detection System/Intrusion Protection System (IDS/IPS) capability to monitor network communications on all networks and subnets of any environment requiring an organization Authority to Operate. a. Permitted IDS/IPS mechanisms: • Centrally managed IDS/IPS devices at network perimeter points, to include between zones; and • Centrally managed host-based IDS/IPS sensor agents in information technology components for which such agents are available. b. Environments where communications within the zone are encrypted must use mechanisms capable of either decrypting content for analysis or analyzing content before transmission/after receipt; and c. Information technology components that do not support host-based IDS/IPS sensors capability must be documented in the applicable risk assessment and security plan. 2. Monitoring functionality supports the sharing of threat awareness information in a format that meets organization requirements. 3. The organization monitors for unauthorized remote connections to the information system continuously, in real-time and takes appropriate action if an unauthorized connection is discovered.
Related Control Requirement(s): AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SI-3, SI-7
Control Implementation Description: "Click here and type text"

14.17.4.1 SI-4 (1): System-Wide Intrusion Detection System

SI-4 (1): System-Wide Intrusion Detection System
Control
The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.17.4.2 SI-4 (4): Inbound and Outbound Communications Traffic

SI-4 (4): Inbound and Outbound Communications Traffic
Control
The information system monitors inbound and outbound communications traffic at a defined frequency (defined in the applicable System Security Plan) for unusual or unauthorized activities or conditions.
Related Control Requirement(s):

SI-4 (4): Inbound and Outbound Communications Traffic
Control Implementation Description:
"Click here and type text"

14.17.4.3 SI-4 (5): System-Generated Alerts

SI-4 (5): System-Generated Alerts
Control
The information system sends alerts to defined personnel or roles (defined in the applicable System Security Plan) when the following indications of compromise or potential compromise occur: a. Presence of malicious code; b. Unauthorized export of information; c. Signaling to an external information system; or d. Potential intrusions. **Implementation Standards** 1. The organization defines additional compromise indicators as needed. 2. The indications that a compromise or potential compromise occurred include: protected information system files or directories have been modified without notification from the appropriate change/configuration management channels; information system performance indicates resource consumption that is inconsistent with expected operating conditions; auditing functionality has been disabled or modified to reduce audit visibility; audit or log records have been deleted or modified without explanation; information system is raising alerts or faults in a manner that indicates the presence of an abnormal condition; resource or service requests are initiated from clients that are outside of the expected client membership set; information system reports failed logins or password changes for administrative or key service accounts; processes and services are running that are outside of the baseline configuration/system profile; utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose.
Related Control Requirement(s):
AU-5, PE-6
Control Implementation Description:
"Click here and type text"

14.17.5 SI-5: Security Alerts, Advisories, and Directives

SI-5: Security Alerts, Advisories, and Directives
Control
The organization: a. Receives information system security alerts, advisories, and directives from defined external organizations (including US-CERT and organizations as defined in the applicable System Security Plan) on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary;

SI-5: Security Alerts, Advisories, and Directives
c. Disseminates security alerts, advisories, and directives to: defined personnel or roles with system administration, monitoring, and/or security responsibilities (defined in the applicable System Security Plan); d. The organization defines a list of personnel (identified by name and/or by role) with system administration, monitoring, and/or security responsibilities who are to receive security alerts, advisories, and directives; and e. Implements security directives in accordance with established timeframes, or notifies the business owner of the degree of noncompliance.
Related Control Requirement(s): SI-2
Control Implementation Description: "Click here and type text"

14.17.6 SI-6: Security Functionality Verification

SI-6: Security Function Verification
Control
The information system: a. Verifies the correct operation of defined security functions (defined in the applicable System Security Plan); b. Performs this verification upon system startup, restart, and upon command by a user with appropriate privileges no less often than once per month; c. Notifies system administration of failed security verification tests; and d. Shuts the information system down, or restarts the information system, or performs some other defined alternative action(s) (defined in the applicable System Security Plan) when anomalies are discovered.
Related Control Requirement(s): CA-7, CM-6
Control Implementation Description: "Click here and type text"

14.17.7 SI-7: Software, Firmware, and Information Integrity

SI-7: Software, Firmware, and Information Integrity
Control
The organization employs integrity verification tools to detect unauthorized changes to software and information.
Related Control Requirement(s): SC-8, SC-13, SI-3
Control Implementation Description: "Click here and type text"

14.17.7.1 SI-7 (1): Integrity Checks

SI-7 (1): Integrity Checks
Control
The organization performs an integrity check of software, firmware, and information daily and at system startup and reassesses the integrity of software and information by performing no less often than one monthly scan of the information system.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.17.7.2 SI-7 (7): Integration of Detection and Response

SI-7 (7): Integration of Detection and Response
Control
The organization employs integrity verification tools to detect unauthorized changes to software, firmware, and information.
Related Control Requirement(s): SC-13, SI-3
Control Implementation Description: "Click here and type text"

14.17.8 SI-8: Spam Protection

SI-8: Spam Protection
Control
The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.
Related Control Requirement(s): AT-2, AT-3, SC-5, SC-7, SI-3
Control Implementation Description: "Click here and type text"

14.17.8.1 SI-8 (2): Automatic Updates

SI-8 (2): Automatic Updates
Control
The information system automatically updates spam protection mechanisms.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.17.9 SI-10: Information Input Validation

SI-10: Information Input Validation
Control
The information system checks the validity of defined information inputs (defined in the System Security Plan) for accuracy, completeness, validity, and authenticity as close to the point of origin as possible and the validity of personally identifiable information (PII) being processed, stored, or transmitted.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.17.10 SI-11: Error Handling

SI-11: Error Handling
Control
The information system: a. Generates error messages that provide information necessary for corrective actions without revealing user name and password combinations; attributes used to validate a password reset request (e.g., security questions); personally identifiable information (excluding unique user name identifiers provided as a normal part of a transactional record); biometric data or personal characteristics used to authenticate identity; sensitive financial records (e.g. account numbers, access codes); content related to internal security functions (i.e., private encryption keys, white list or blacklist rules, object permission attributes and settings in error logs and administrative messages that could be exploited by adversaries.; and b. Reveals error messages only to defined personnel or roles (defined in the System Security Plan). c. Reveals error messages only to authorized individuals with a need for the information in the performance of their duties.
Related Control Requirement(s): AU-2, AU-3, SI-2
Control Implementation Description: "Click here and type text"

14.17.11 SI-12: Information Handling and Retention

SI-12: Information Handling and Retention
Control
The organization handles and retains information within the information system and information output from the system in accordance with applicable state and federal laws directives, policies, regulations, standards, and operational requirements. **Implementation Standard** Retain output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system for ten (10) years or in accordance with organizational requirements, whichever is more restrictive.
Related Control Requirement(s): AU-5, AU-11, MP-2, MP-4, AP-2, DM-2
Control Implementation Description: "Click here and type text"

14.17.12 SI-16: Memory Protection

SI-16: Memory Protection
Control
The information system implements security safeguards (e.g., data execution prevention, address space layout randomization) to protect its memory from unauthorized code execution. Implemented safeguards must be specified in the applicable system security plan.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"

14.18 Authority and Purpose (AP)

14.18.1 AP-1: Authority to Collect

AP-1: Authority to Collect
Control
The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of Personally Identifiable Information (PII), either generally or in support of a specific program or information system need.

AP-1: Authority to Collect
Related Control Requirement(s): AR-2, DM-1, TR-1
Control Implementation Description "Click here and type text"

14.18.2 AP-2: Purpose Specification

AP-2: Purpose Specification
Control
The organization describes the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices and data sharing agreements.
Related Control Requirement(s): AR-2, AR-4, AR-5, DM-1, DM-2, TR-1, UL-1, UL-2
Control Implementation Description "Click here and type text"

14.19 Accountability, Audit, and Risk Management (AR)

14.19.1 AR-1: Governance and Privacy Program

AR-1: Governance and Privacy Program
Control
The organization: a. Appoints a designated privacy official accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems; b. Monitors federal (and state as applicable)] privacy laws and policy for changes that affect the privacy program; c. Allocates appropriate budget and staffing resources to implement and operate the organization-wide privacy program; d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures; e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and f. Updates the privacy plan, policies, and procedures, as required to address changing requirements, but no less often than every two years. **Implementation Standard** Development of the strategic organizational privacy plan must be done in consultation with the organization CIO and CISO. The organization establishes and institutionalizes contact for its privacy professionals with selected groups and associations within the privacy community:

AR-1: Governance and Privacy Program
a. To facilitate ongoing privacy education and training for organizational personnel; b. To maintain currency with recommended privacy practices, techniques, and technologies; and c. To share current privacy-related information including threats, vulnerabilities, and incidents.
Related Control Requirement(s):
Control Implementation Description "Click here and type text"

14.19.2 AR-2: Privacy Impact and Risk Assessment

AR-2: Privacy Impact and Risk Assessment
Control
The organization: a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, storage, sharing, transmitting, use, and disposal of PII; and b. Conducts privacy impact assessments for information systems, programs, or other activities that pose a risk to the privacy of PII. c. Reviews the PIA no less than every three (3) years or when major systems changes occur.
Related Control Requirement(s): SE-2
Control Implementation Description «Click here and type text.]»

14.19.3 AR-4: Privacy Monitoring and Auditing

AR-4: Privacy Monitoring and Auditing
Control
The organization: a. Monitors and audits privacy controls no less often than once every 365 days to ensure effective implementation; and b. Monitors for changes to applicable privacy laws, regulations, and policy affecting internal privacy policy no less often than once every 365 days to ensure internal privacy policy remains effective; and c. Documents, tracks, and ensures mitigation of corrective actions identified through monitoring or auditing.
Related Control Requirement(s): AR-7, AU-1, AU-2, AU-3, AU-6, AU-12, CA-7, TR-1, UL-2
Control Implementation Description "Click here and type text"

14.19.4 AR-5: Privacy Awareness and Training

AR-5: Privacy Awareness and Training
Control
The organization: d. Develops, implements, and updates a comprehensive privacy training and awareness strategy aimed at ensuring personnel understand privacy responsibilities and procedures; e. Administers basic privacy training no less often than once every three hundred sixty-five (365) days, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII no less often than once every three hundred sixty-five (365) days; and f. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements no less often than once every three hundred sixty-five (365) days. **Implementation Standards** 1. A privacy education and awareness training program must be developed and implemented for all employees and individuals working on behalf of the organization involved in managing, using, and/or processing PII. 2. Privacy education and awareness training must include responsibilities associated with sending PII in email. 3. Communications and training related to privacy and security must be job-specific and commensurate with the employee's responsibilities. 4. Agencies must initially train employees (including managers) on their privacy and security responsibilities before permitting access to organization information and information systems. Thereafter, agencies must provide at least annual refresher training to ensure employees continue to understand their responsibilities. 5. Additional or advanced training must be provided commensurate with increased responsibilities or change in duties. 6. Both initial and refresher training must include acceptable rules of behavior and the consequences when the rules are not followed. 7. Training must address the rules for telework and other authorized remote access programs.
Related Control Requirement(s): AT-2, AT-3, AT-4, TR-1
Control Implementation Description "Click here and type text"

14.19.5 AR-7: Privacy-Enhanced System Design and Development

AR-7: Privacy-Enhanced System Design and Development
Control
The organization: a. Designs information systems that support privacy with automated privacy controls. b. Conducts periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act, the organization's privacy policy, and any other legal or regulatory requirements.

AR-7: Privacy-Enhanced System Design and Development
Related Control Requirement(s): AC-6, AR-4, AR-5, DM-2, TR-1, SA-3
Control Implementation Description "Click here and type text"

14.19.6 AR-8: Accounting of Disclosures

AR-8: Accounting of Disclosures
Control
The organization: a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including: 1. Date, nature, and purpose of each disclosure of a record; and 2. Name and address of the person or agency to which the disclosure was made. b. Retains the accounting of disclosures for the life of the record or ten (10) years after the disclosure is made, whichever is longer; and c. Makes the accounting of disclosures available to the person named in the record upon request.
Related Control Requirement(s): IP-2, AU-2, AU-3, AU-11
Control Implementation Description "Click here and type text"

14.20 Data Quality and Integrity (DI)

14.20.1 DI-1: Data Quality

DI-1: Data Quality
Control
The organization: a. Confirms to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information; b. Collects PII directly from the individual to the greatest extent practicable; c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems no less often than once every 365 days; and d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

DI-1: Data Quality
Related Control Requirement(s): AP-2, DM-1, IP-3 SI-10
Control Implementation Description "Click here and type text"

14.20.1.1 DI-1 (1): Validate PII

DI-1 (1): Validate PII
Control
The organization requests the individual or the individual's authorized representative validate PII during the collection process.
Related Control Requirement(s): AP-2, DM-1, IP-3, SI-10
Control Implementation Description "Click here and type text"

14.21 Data Minimization and Retention (DM)

14.21.1 DM-1: Minimization of Personally Identifiable Information

DM-1: Minimization of Personally Identifiable Information
Control
The organization: a. Identifies the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection; b. Limits the collection and retention of PII to the minimum elements identified, for the purposes described in the notice, and for which the individual has provided consent; and c. Conducts an initial evaluation of PII holdings, and establishes and follows a schedule for regularly reviewing those holdings, no less often than once every three hundred sixty-five (365) days, to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.
Related Control Requirement(s): AP-1, AP-2, AR-4, IP-1, SE-1, SI-12, TR-1
Control Implementation Description "Click here and type text"

14.21.1.1 DM-1 (1): Locate / Remove / Redact / Anonymize PII

DM-1 (1): Locate / Remove / Redact / Anonymize PII
Control
The organization, where feasible and within the limits of technology and the law, locates, and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.
Related Control Requirement(s): AP-1, AP-2, AR-4, IP-1, SE-1, SI-12, TR-1
Control Implementation Description "Click here and type text"

14.21.2 DM-2: Data Retention and Disposal

DM-2: Data Retention and Disposal
Control
The organization: a. Retains each collection of PII for the time period specified by the NARA-approved Records Schedule in consultation with the Records Management Officer to fulfill the purpose(s) identified in the notice or as required by law; b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and c. Uses FIPS-validated techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).
Related Control Requirement(s): AR-4, AU-11, DM-1, MP-1, MP-3, MP-4, MP-5, MP-6, MP-7, SI-12, TR-1
Control Implementation Description "Click here and type text"

14.21.2.1 DM-2 (1): System Configuration

DM-2 (1): System Configuration
Control
The organization, where feasible, configures information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under a NARA-approved Records Schedule.

DM-2 (1): System Configuration
Related Control Requirement(s): AR-4, AU-11, DM-1, MP-1, MP-3, MP-4, MP-5, MP-6, MP-7, SI-12, TR-1
Control Implementation Description "Click here and type text"

14.21.3 DM-3: Minimization of PII Used in Testing, Training, and Research

DM-3: Minimization of PII Used in Testing, Training, and Research
Control
The organization: a. Develops policies and procedures that minimize the use of PII for testing,training, and research; and b. Implements controls to protect PII used for testing, training, and research. To the greatest extent possible, PII should not be used when testing or developing an information system.
Related Control Requirement(s):
Control Implementation Description "Click here and type text"

14.21.3.1 DM-3 (1): Risk Minimization Techniques

DM-3 (1): Risk Minimization Techniques
Control
The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.
Related Control Requirement(s):
Control Implementation Description "Click here and type text"

14.22 Individual Participation and Redress (IP)

14.22.1 IP-1: Consent

IP-1: Consent
Control
The organization: a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintenance, and sharing of PII prior to its collection;

IP-1: Consent
b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, or retention of PII; c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosures of previously collected PII; and d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice and any relevant business agreements that were in effect at the time the organization collected the PII. e. Consent documents must be appropriately secured and retained for ten (10) years.
Related Control Requirement(s): AC-2, AP-1, TR-1
Control Implementation Description "Click here and type text"

14.22.2 IP-2: Individual Access

IP-2: Individual Access
Control
The organization: a. Provides individuals the ability to have access to their PII maintained in its system(s) of records; b. Publishes policies and/or regulations governing how individuals may request access to records maintained in the system of records; c. Publishes access procedures; and d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.
Related Control Requirement(s): AR-8, IP-3, TR-1
Control Implementation Description "Click here and type text"

14.22.3 IP-3: Redress

IP-3: Redress
Control
The organization: a. Provides a process for individuals to have inaccurate, incomplete or out-of-date PII maintained by the organization corrected, substituted, deleted,or amended, as appropriate; and b. Establishes a process for disseminating corrections or amendments of the PII, if the inaccurate PII was maintained solely by the organization, to other authorized users of the PII, such as external information. sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

IP-3: Redress
Related Control Requirement(s): IP-2, TR-1, UL-2
Control Implementation Description "Click here and type text"

14.22.4 IP-4: Complaint Management

IP-4: Complaint Management
Control
The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.
Related Control Requirement(s): IP-3
Control Implementation Description "Click here and type text"

14.22.4.1 IP-4 (1): Response Times

IP-4 (1): Response Times
Control
The organization: a. Acknowledges complaints, concerns, or questions from individuals within ten (10) working days; b. Completes review of requests within thirty (30) working days of receipt, unless unusual or exceptional circumstances preclude completing action by that time; and c. Responds to any appeal as soon as possible, but no later than thirty (30) working days after receipt of the appeal unless the appeal authority can show good cause to extend the response period.
Related Control Requirement(s):
Control Implementation Description "Click here and type text"

14.23 Security (SE)

14.23.1 SE-1: Inventory of Personally Identifiable Information

SE-1: Inventory of Personally Identifiable Information
Control
The organization:

SE-1: Inventory of Personally Identifiable Information
a. Establishes, maintains, and updates, no less often than once every 365 days, an inventory of all programs and systems used for collecting, creating, using, disclosing, maintaining, or sharing PII; and b. Provides each update of the PII inventory to the organization's designated senior privacy official or chief information security official no less often than once every three hundred sixty-five 365 days to support the establishment of information security requirements for all new or modified information systems containing PII.
Related Control Requirement(s): AR-1, AR-4, AR-5, AT-1, DM-1
Control Implementation Description "Click here and type text"

14.23.2 SE-2: Privacy Incident Response

SE-2: Privacy Incident Response
Control
The organization: a. Develops and implements a Privacy Incident and Breach Response Plan; b. Provides an organized and effective response to privacy incidents and breaches in accordance with the organizational Privacy Incident and Breach Response Plan; and c. Require reporting of any security and privacy Incident or Breach of PII to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at cms_it_service_desk@cms.hhs.gov within one hour after discovery of the Incident or Breach.
Related Control Requirement(s): AR-1, AR-4, AR-5, AU-1 through AU-12, IR-2, IR-4, IR-6, IR-8, RA-1
Control Implementation Description "Click here and type text"

14.24 Transparency (TR)

14.24.1 TR-1: Privacy Notice

TR-1: Privacy Notice
Control
The organization: a. Provides effective notice to the public and to individuals regarding: 1. Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII; 2. Authority for collecting PII; 3. The choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and 4. The ability to access and have PII amended or corrected if necessary.

TR-1: Privacy Notice
b. Describes: 1. The PII the organization collects and the purpose(s) for which it collects that information; 2. How the organization uses PII internally; 3. Whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; 4. Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; 5. How individuals may obtain access to PII; and 6. How the PII will be protected. c. Maintain its Privacy Notice statement content by reviewing and revising as necessary on an annual basis, at a minimum, and before or as soon as possible after any change to its privacy policies and procedures.
Related Control Requirement(s): AP-1, AP-2, AR-1, AR-2, IP-1, IP-2, IP-3, UL-1, UL-2
Control Implementation Description "Click here and type text"

14.24.2 TR-3: Dissemination of Privacy Program Information

TR-3: Dissemination of Privacy Program Information
Control
The organization: a. Ensures the public has access to information about its privacy activities and is able to communicate with its designated privacy official. b. Ensures its privacy and security practices are publicly available through organizational websites or otherwise and provide information on how to file complaints.
Related Control Requirement(s): AR-6
Control Implementation Description "Click here and type text"

14.25 Use Limitation (UL)

14.25.1 UL-1: Internal Use

UL-1: Internal Use
Control
The organization uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices as well as in applicable contractural agreements.

UL-1: Internal Use
Related Control Requirement(s): AP-2, AR-2, AR-4, AR-5, IP-1, TR-1
Control Implementation Description "Click here and type text"

14.25.2 UL-2: Information Sharing with Third Parties

UL-2: Information Sharing with Third Parties
Control
The organization: a. Shares PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements (CMAs), or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required. **Implementation Standard** Consistent with the Purpose Specification and Use Limitation Fair Information Practice Principles (FIPPs), sharing of PII must be compatible with the purpose for which it was collected. Consistent with the Transparency FIPP, any subsequent sharing that is not compatible may not be done until additional notice is provided to the individual, their consent is obtained, and relevant documents are updated or published; e.g., when applicable and appropriate, publish an updated system of records notice (SORN) to cover the additional incompatible sharing and obtain consent from the affected individuals.
Related Control Requirement(s): AR-3, AR-4, AR-5, AR-8, AP-2, DI-1, IP-1, TR-1
Control Implementation Description "Click here and type text"

15. Systems Security Plan Attachments

Instruction: As part of the information systems development life cycle management process, specific security and privacy artifacts are required, including the System Security Plan (SSP). The following attachments represent the security and privacy artifacts that should be developed and maintained during the life cycle management process of information systems. They should be developed and maintained as separate documents, however, these documents should be included as part of the SSP for future evaluation purposes. Maintaining these documents as attachments facilitates version control of all related materials.

The NEE security control requirement, CA-2, requires that assessments be conducted by independent assessors or third-party assessors. The assessments include reviews of the organizational security and privacy program, policies and guidance, network and component scanning, configuration assessments, and documentation reviews. Consequently, many of the attached documents should be available for review during these annual assessments.

Attach any documents that are referred to in the <Information System Name> System Security Plan. Documents and attachments should provide the title, version. and exact file name, including the file extension. All attachments and associated documents must be delivered separately. No embedded documents will be accepted.

Delete this and all other instructions from your final version of this document.

Table 15-1 provides recommended file naming conventions for the attachments to the SSP. A Use this to generate names for the attachments. Make only the following additions/changes to Table 15-1:

- The first item, Information Security Policies and Procedures (ISPP), may be fulfilled by multiple documents. If that is the case, add lines to Table 15-1Table 15-1 to differentiate them using the "ISP" portion of the File Name. *Example* <Information System Abbreviation> *A1 ISPP xx v1.0*. Delete the "xx" if there is only one document.
- Enter the file extension for each attachment.
- Do not change the Version Number in the File Name in Table 15-1 (Information System Abbreviation, attachment number, document abbreviation, version number)

Table 15-1. Attachment File Naming Convention

Attachment	File Name	File Extension
Information Security Policies and Procedures	<Information System Abbreviation> A1 ISPP xx v1.0	. enter extension
Information System Documentation	<Information System Abbreviation> A2 ISD v1.0	. enter extension

Attachment	File Name	File Extension
E-Authentication Worksheet	Included in Attachment 3 – e-Authentication Worksheet	
PIA	<Information System Abbreviation> A4 PIA v1.0	. enter extension
Rules of Behavior	<Information System Abbreviation> A5 ROB v1.0	. enter extension
Information System Contingency Plan	<Information System Abbreviation> A6 ISCP v1.0	. enter extension
Configuration Management Plan	<Information System Abbreviation> A7 CMP v1.0	. enter extension
Equipment List	<Information System Abbreviation> A8 INVE	. enter extension
Software List	<Information System Abbreviation> A9 INVS	. enter extension
Detailed Configuration Settings	<Information System Abbreviation> A10 CM	. enter extension
Incident Response Plan	<Information System Abbreviation> A11 IRP v1.0	. enter extension
Applicable Laws, Regulations, Standards, and Guidance	<Information System Abbreviation> A12 REG v1.0	. enter extension
Security and Privacy Agreements and Compliance Artifacts	<Information System Abbreviation> A13 COM v1.0	. enter extension
Acronyms	<Information System Abbreviation> A14 AYM	. enter extension

15.1 Attachment 1 – Information Security Policies and Procedures

This section should contain a list of all policies and procedures related to the implementation of security and privacy controls for the NEE system or that is referenced as part of the system security plan. This list should include the title of the document(s), their most recent dates, and version # (if applicable). These policies and procedures will be reviewed as part of the annual third-party independent assessments.

15.2 Attachment 2 – Information System Documentation

The NEE security control, SA-5, Information System Documentation, requires the development and implementation of documentation used to support the maintenance and operation of the information system. This documentation includes administrator documentation, user documentation, and system documentation. This attachment contains a list of this documentation, including where it is maintained.

15.3 Attachment 3 – E-Authentication Worksheet

Instruction: This Attachment Section has been revised to include the E-Authentication template. Therefore, a separate attachment is not needed.

[Delete this note and all other instructions from your final version of this document.]

15.3.1 FFE Partner Identity Proofing Requirements

The FFE Partner must use the FFE's Remote Identity Proofing service from the Hub for consumers. If the FFE Partner uses a different third-party identity proofing service, the service must be Federated Identity, Credential, and Access Management (FICAM) Trust Framework Solutions (TFS) approved, and the FFE Partner must be able to produce documentary evidence that each applicant has been successfully identity proofed.

Electronic Authentication (E-Authentication) is the process of establishing confidence in user identities electronically presented to an information system. The E-Authentication section explains the objective for selecting the appropriate e-Authentication level for the candidate system. Guidance on selecting the system authentication technology solution is available in NIST SP 800-63, Revision 3, *Digital Identity Guidelines*. Authentication focuses on confirming a person's identity, based on the reliability of his or her credential. Office of Management and Budget (OMB) Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, requires federal information system owners to determine the system's electronic authentication requirements to minimize the potential impact of authentication errors and misuse of credentials.

In accordance with Executive Order 13681, making PII accessible through digital applications requires the use of multi-factor authentication and an effective identity proofing process as appropriate. It is strongly recommended that FFE Partner leverage multi-factor authentication.

15.3.2 Information System Name / Title

This E-Authentication Plan provides an overview of the security requirements for the <Information System Name> in accordance with OMB Memorandum M-04-04.

Table 15-2. Information System Name and Title

Information System Name	Information System Abbreviation
<Information System Name>	<Information System Abbreviation>

15.3.3 E-Authentication Level Definitions

NIST SP 800-63-3,[1] *Digital Identity Guidelines*, applies to all online transactions that require digital identity and/or authentication that are accessed by the general public, government entities, government employees, business partners, and contractors. NIST SP 800-63-3 applies to internal-facing systems accessed by employees and contractors, public-facing Internet accessible systems, and mobile devices (e.g., smartphones and tablets) whether accessed via browsers, applications, mobile apps, or operating systems.

Contrary to earlier versions of NIST SP 800-63, the current guidance no longer calls for a single composite assurance level for identification and authentication. Instead, a risk-based approach is used to determine three (possibly different) assurance levels:

- An identification assurance level (IAL) corresponding to the strength (aka robustness) of the identity proofing process;
- An authentication assurance level (AAL) corresponding to the strength of the authentication process; and
- A federated assurance level (FAL) corresponding to the strength of the assertion protocol used in federated environments to communicate authentication and attribute information to a relying party (RP). (**Note:** This only applies to federated architectures.)

For non-federated identity and authorization systems, only the IAL and AAL are required; for federated digital identity systems, the IAL, AAL, and FAL must be selected.

The Three E-Authentication Assurance Levels

The requirements for the identity assurance levels are described in NIST SP 800-63-3, Table 5-1, and are summarized as follows:

- IAL1 permits the individual's attributes to be self-asserted.
- IAL2 requires the individual's identifying attributes to be verified in person or remotely.
- IAL3 requires the individual's identity to be verified in-person through examination of their physical documentation.

The requirements for the authenticator assurance levels are described in NIST SP 800-63-3, Table 5-2, and are summarized as follows:

- AAL1 requires **single-factor authentication** and that the claimant prove possession and control of the authenticator(s) through a secure authentication protocol;
- AAL2 requires **two-factor authentication** and that the claimant prove possession and control of two different authentication factors through a secure authentication protocol and using approved cryptographic techniques.[2]

---

[1] Located at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

[2] Examples of two-factor/multi-factor authentication include a combination of two or more of the following: something you have (e.g., PIV card, hardware token, etc.), something you know (e.g., password, pin, etc.), and something you are (e.g., biometrics, such as iris scan, finger prints, etc.).

- Similar to AAL2, AAL3 requires **two-factor authentication** and that the claimant prove possession and control of two different authentication factors through a secure authentication protocol and using approved cryptographic techniques. In addition, AAL3 requires the claimant prove possession of a key authenticator (i.e., hardware token) that uses a cryptographic protocol as one of the authentication factors.

The requirements for the federation assurance levels are described in NIST SP 800-63-3, Table 5-3, and are summarized as follows:

- FAL1 permits the identity provider (IdP) to present (and the RP to receive) a digitally signed bearer assertion to the RP; the digital signature must use approved cryptography;
- FAL2 requires that the assertion be encrypted using approved cryptography that ensures that only the RP can decrypt it; and
- FAL3 requires the subscriber to present proof of possession of a cryptographic key reference (i.e., hardware token) in the assertion in addition to the assertion artifact itself. The assertion must be signed by IdP and encrypted to the RP using approved cryptography.

NIST SP 800-63A includes specific requirements for implementing each IAL level, NIST SP 800-63B specifies the requirements for implementing each AAL level, and NIST SP 800-63C defines the requirements for implementing each FAL level.

For each of the three assurance levels (IAL, AAL, FAL), the system owner is required to evaluate the potential consequences if the processes for identifying and authenticating an individual do not function properly (e.g., if individuals using false identities and/or incorrect authenticators are authenticated by the system) by assessing six categories of potential harm and impact:

1. Inconvenience, distress, or damage to standing or reputation;
2. Financial loss or agency liability;
3. Harm to agency programs or public interests;
4. Unauthorized release of sensitive information;
5. Personal safety; and
6. Civil or criminal violations.

For each of these six categories of harm and impact, the potential impact values that may be specified are low, moderate, and high impact. The assessment should only be made for the online transactions portion of the system and should not include offline business processes or online processing that is part of a different completely segmented system (please refer to NIST SP 800-63-3 Section 5.3.1). In particular, Section 5.3.1 states:

> The assurance level determination is only based on transactions that are part of a digital system. An online transaction may not be equivalent to a complete business process that requires offline processing, or online processing in a completely segmented system. In selecting the appropriate assurance levels, the agency should assess the risk associated

with online transactions they are offering via the digital service, not the entire business process associated with the provided benefit or service.

Table 15-3 specifies the impact values for the six impact categories that are permitted for each assurance level (note that Table 15-3 is derived from NIST SP 800-63-3 Table 6-1). The assurance level selected should be the lowest level whose impact profile meets or exceeds the potential impact for every category analyzed in the risk assessment (e.g., "high water mark").

Table 15-3. Maximum Potential Impacts for Each of the Three Assurance Levels (IAL, AAL, and FAL)

Impact Categories	Assurance Level 1	Assurance Level 2	Assurance Level 3
Inconvenience, distress or damage to standing or reputation	Low	Moderate	High
Financial loss or agency liability	Low	Moderate	High
Harm to agency programs or public interests	N/A	Low or Moderate	High
Unauthorized release of sensitive information	N/A	Low or Moderate	High
Personal Safety	N/A	Low	Moderate or High
Civil or criminal violations	N/A	Low or Moderate	High

The assurance levels for IAL, AAL, and FAL may differ—they are not required to be the same. In addition, the NEE may require a higher assurance level than the level derived from the methodology described in NIST SP 800-63-3 and this document. If an assurance level is selected that differs from the level that results from following the NIST process, the justification for deviating from the derived assurance level must be documented and included.

15.3.4 E-Authentication Level Selection

Instruction: Indicate the IAL, AAL, FAL assurance levels and authentication type used for each user role in the cell for Response Data in Table 15-4Table 15-4.

[Delete this instruction from your final version of this document.]

Implementation details of the E-Authentication mechanisms are provided in the SSP under security control IA-2.

Table 15-4. E-Authentication Assurance Levels and Authentication Solutions

User Role	Assurance Level	Authentication Type
Example: Anonymous Shopper	IAL1	None
Example: Agents and Brokers	IAL2, AAL1	SAML; Username/Password
Example: NEE Administrators	IAL3, AAL-2	SAML; Username/Password and 2FA

15.4 Attachment 4 – PIA

Instruction: This Attachment Section should contain a completed Privacy Impact Assessment (PIA) as required by the privacy control, AR-2. CMS provided an EDE PIA template. Application-specific PIAs are required for each system connection to the Hub. They must also be reviewed as part of the annual independent third-party audits.

[Delete this note and all other instructions from your final version of this document.]

A completed and up-to-date PIA is required for connection to the Hub.

15.4.1 Privacy Overview and Point of Contact (POC)

Table 15-5 identifies the individual who serves as the System Name Privacy Officer and POC for privacy at Non-Exchange Entity.

Table 15-5. System Name Privacy POC

Privacy POC Information	Detail
Name	Click here to enter text.
Title	Click here to enter text.
PARTNER / Organization	Click here to enter text.
Address	Click here to enter text.
Phone Number	Click here to enter text.
Email Address	Click here to enter text.

15.4.1.1 Personally Identifiable Information (PII)

Personally Identifiable Information (PII), as defined in OMB Memorandum M-07-16, refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Information that could be tied to more than one person (date of birth) is not considered PII unless it is made available with other types of information that together could render both values as PII (for example, date of birth and street address). A non-exhaustive list of examples of types of PII includes:

- Social Security numbers

- Passport numbers
- Driver's license numbers
- Biometric information
- DNA information
- Bank account numbers

PII does not refer to business information or government information that cannot be traced back to an individual person.

15.5 Attachment 5 – Rules of Behavior

The Rules of Behavior (RoB) describes controls associated with user responsibilities and certain expectations of behavior for following security policies, standards and procedures. Security control PL-4 requires a PARTNER to implement rules of behavior.

The Rules of Behavior should be aligned with the DHHS rules of behavior that are posted at: http://www.hhs.gov/ocio/policy/hhs-rob.html.

15.6 Attachment 6 – Information System Contingency Plan

This attachment should contain the information system contingency plan. The NEE security control, CP-2, requires that an organization develop a contingency plan for its information systems and applications. Security control CP-3, Contingency Training, requires organizations to ensure that the key stakeholders of contingency planning are appropriately trained. Security control CP-4 requires organizations to ensure that the contingency plans are tested to determine the effectiveness of the plans and to identify potential weaknesses in the plans. The contingency plan must be in place before connection to the Hub. It should also be available for review as part of the annual independent third-party assessment.

The contingency plan that meets the security control CP-2 requirements should be developed in accordance with NIST SP 800-34.

15.7 Attachment 7 – Configuration Management Plan

This attachment should contain the Configuration Management Plan. Security control, CM-9, requires organizations to develop, document, and implement a configuration management plan for the information system/application. Configuration management plans are required to be developed and implemented to support the management of all configuration items supporting the information system/application. NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011, provides guidance for developing the configuration management plan.

15.8 Attachment 8 – Equipment List

This attachment contains a listing of equipment that supports the system/application. This list should be consistent with requirements included in the CM-8 control family (Information System Component Inventory) and associated implementation standards.

15.9 Attachment 9 – Software List

This attachment contains a listing of software that supports the system/application. This list should be consistent with the requirements included in the CM-8 control family (Information System Component inventory) and associated implementation standards.

15.10 Attachment 10 – SSP Detailed Configuration Setting Standards

This attachment contains the detailed configuration setting standards that satisfy the required system baseline configurations. These settings should be consistent with the requirements of security controls CM-2 and CM-6 and associated implementation standards.

15.11 Attachment 11 – Incident Response Plan

This attachment should contain the documented Incident Response Plan, which must be consistent with CMS Incident and Breach Notification Procedures within the CMS *Risk Management Handbook*.[3] The NEE security control, IR-8, requires the development and implementation of an Incident Response Plan that provides a standard road map for implementing incident response. Also, the privacy control, SE-2, requires the implementation of a Privacy Incident and Breach Response Plan that is required to focus on developing a risk-based approach for privacy breaches and to ensure consistency in the reporting of privacy breach notifications. Organizations have the option of integrating the Privacy Incident Response Plan with their Security Incident Response Plan or keeping the plans separate. The objective is to ensure the implementation of the control requirements associated with both plans. The Incident Response Plan(s) must be in place before connection to the CMS Federal Data Services Hub and are artifacts that should be available for review as part of the annual Third-Party Independent Assessment.

[3] Located at: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-8-Incident-Response.pdf

15.12 Attachment 12 – Applicable Laws, Regulations, Standards, and Guidance

By interconnecting with the CMS network and CMS information system, the Non-Exchange Entity agrees to be bound by the Interconnection Security Agreement (ISA) and the use of the CMS network and information system in compliance with the ISA. Laws and regulations and standards that apply include the following:

- Federal Information Security Management Act of 2014 (FISMA)
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems
- 18 U.S.C. § 641 Criminal Code: Public Money, Property or Records
- 18 U.S.C. § 1905 Criminal Code: Disclosure of Confidential Information
- Privacy Act of 1974, 5 U.S.C. § 552a
- Health Insurance Portability and Accountability Act (HIPAA) of 1966 P.L. 104-191
- Patient Protection and Affordability Care Act ("PPACA") of 2010
- HHS Regulation 45 CFR §155.260 – Privacy and Security of Personally Identifiable Information
- HHS Regulation 45 CFR §155.280 – Oversight and monitoring of privacy and security requirements
- NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*

CMS has provided, within its system security and privacy oversight capacity, the following guidance documents and templates:

- Framework for Independent Assessment of Security and Privacy Controls for NEEs
- CMS Interconnection Security Agreement (ISA) for NEEs
- Security and Privacy Controls Assessment Test Plan (SAP) template
- Security and Privacy Assessment Report (SAR) template
- NEE System Security and Privacy Plan (SSP) workbook
- Plan of Action & Milestones (POA&M) template
- Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide

15.13 Attachment 13 – Security and Privacy Agreements and Compliance Artifacts

The NEEs and their business partners are required to manage their information system(s) using an organizationally defined system development life cycle (SDLC) that integrates security and privacy into the development, implementation, and operation of the information system and continues through maintenance and disposal. This attachment provides a list of required security and privacy agreements and compliance artifacts (as shown in Table 15-6) that either must be submitted to CMS, must be in place before connecting to the Hub, or are required to be reviewed during annual third-party independent security assessments of NEE information systems/applications.

Table 15-6. Required Security and Privacy Agreements and Compliance Artifacts

Artifact Title	Required Before Connection to the Hub	Required for Independent Audit Every Year	Required for Continuous Monitoring and Updates	Required to Be Delivered to CMS
Privacy Impact Assessment (PIA) – Application-specific for each NEE IT System	Yes; self-assessment	Yes	Annual updates	No
Business Agreement with Data Use Agreement (DUA) elements integrated	Yes	Yes	Annual updates	Yes
Interconnection Security Agreement (ISA)	Yes	No	Annual updates	Yes
Plan of Action and Milestones (POA&M)	Yes	Yes	Monthly updates as appropriate	Yes
Final System Security Plan (SSP)	Yes	Yes	Annual updates	No
Security and Privacy Controls Assessment Test Plan (SAP)	Yes	Yes	Annual updates	Yes
Third-Party Independent Security and Privacy Assessment Report (SAR)	Yes	Yes	Annual[4] and in instances of a significant information system change	Yes
Incident Response Plan and Incident / Breach Notification	Yes	Yes	Annual updates	No
Contingency Plan	Yes	Yes	Annual updates	No
Configuration Management Plan	Yes	Yes	Update as needed	No

[4] Please refer to the Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide.

Appendix A. List of Acronyms

Term	Definition
AAL	Authentication Assurance Level
AC	Access Control, a Security Control family
ACL	Access Control List
ACA	Patient Protection and Affordable Care Act of 2010
AO	Authorizing Official
AP	Authority and Purpose, a Privacy Control family
API	Application Programming Interface
AR	Accountability, Audit, and Risk Management, a Privacy Control family
AT	Awareness and Training, a Security Control family
ATO	Authorization to Operate
AU	Audit and Accountability, a Security Control family
BCP	Business Continuity Plan
BPA	Blanket Purchase Agreement
CA	Security Assessment and Authorization, a Security Control family
CE	Control Enhancement
CFR	Code of Federal Regulation
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management, a Security Control family
CMS	Centers for Medicare & Medicaid Services
COTS	Commercial Off-the-Shelf
CP	Contingency Planning, a Security Control family
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security

Term	Definition
DI	Data Quality and Integrity, a Privacy Control family
DISA	Defense Information Systems Agency
DM	Data Minimization and Retention, a Privacy Control family
DNS	Domain Name System
DR	Disaster Recovery, a Security Control family
DRP	Disaster Recovery Plan
EDE	Enhanced Direct Enrollment
EHR	Electronic Healthcare Record
FAL	Federated Assurance Level
FFE	Federally-facilitated Exchange
FICAM	Federal Identity, Credential and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FTP	File Transfer Protocol
GMT	Greenwich Meridian Time
GSS	General Support System
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HTTP	Hypertext Transfer Protocol
Hub	CMS Data Services Hub
IA	Identification and Authentication, a Privacy Control family
IAL	Identification Assurance Level
IdP	Identity Provider
ID	Identity
IDS	Intrusion Detection System
IP	Internet Protocol
IP	Individual Participation and Redress, a Privacy Control family
IPS	Intrusion Prevention System
IR	Incident Response, a Privacy Control family
ISCM	Information Security Continuous Monitoring

Term	Definition
IS	Information System
ISA	Interconnection Security Agreement
IT	Information Technology
MA	Maintenance, a Security Control family
MAC	Media Access Control
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Media Protection, a Security Control family
MTD	Maximum Tolerable Downtime
NARA	National Archives and Records Administration
NEE	Non-Exchange Entity
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
OMB	Office of Management and Budget
PDF	Portable Document Format
PE	Physical and Environmental Protection, a Security Control family
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PL	Planning, a Security Control family
PM	Program Management, a Security Control family
POA&M	Plan of Action & Milestones
PS	Personnel Security, a Security Control family
Pub	Publication
RA	Risk Assessment, a Security Control family
RP	Relying Party
RTO	Recovery Time Objectives
SA	System and Services Acquisition, a Security Control family
SAP	Security and Privacy Controls Assessment Test Plan

Term	Definition
SAR	Security and Privacy Assessment Report
SC	System and Communications Protection, a Security Control family
SCAP	Security Content Automation Protocol
SDLC	System Development Life Cycle
SE	Security, a Privacy Control family
SI	System and Information Integrity, a Security Control family
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SNA	Systems Network Architecture (IBM)
SOC	Security Operations Center
SOP	Senior Official for Privacy
SORN	System of Record Notice
SP	Special Publication
SSP	System Security and Privacy Plan
STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol
TR	Transparency, a Privacy Control family
UL	Use Limitation, a Privacy Control family
URL	Universal Resource Locator
USB	Universal Serial Bus
U.S.C.	United States Code
US-CERT	United States Computer Emergency Response Team
USGCB	United States Government Configuration Baseline
UTC	Universal Time Coordinate
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAP	Wireless Access Point